DATA TRANSMISSION CONTROLLING METHOD

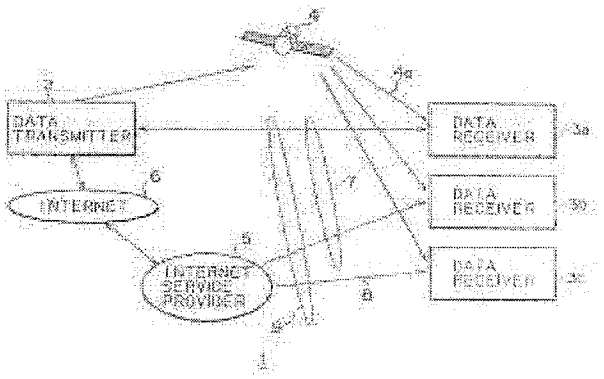
Publication number: KR20060093080 (A)
Publication date: 2006-08-23
Inventor(s): HARA KAZUHIRO [JP]
Applicant(s): SONY CORP [JP]
Classification:
- international: ***G06F13/00; H04L9/28; H04H20/00; H04H20/74; H04H60/23; H04H60/82; H04H60/93; H04L9/00; H04L9/08; H04L9/14; H04L29/06; H04L29/08; H04N7/16; H04N7/167;*** **G06F13/00; H04L9/28; H04H1/00; H04L9/00; H04L9/08; H04L9/14; H04L29/06; H04L29/08; H04N7/16; H04N7/167**
- European: H04L9/08; H04L29/06S4B
Application number: KR20060062089 20060703
Priority number(s): JP19980129214 19980512

Also published as:
EP0957606 (A2)
EP0957606 (A3)
KR20060086337 (A)
JP11331310 (A)
CN1645865 (A)

Abstract not available for KR 20060093080 (A)
Abstract of corresponding document: **EP 0957606 (A2)**

A data transmission system permits secure and more reliable transmission of data from a data transmitter (2) to a data receiver or receivers (3a, 3b, 3c). The system comprises: a data transmitter (2) for encrypting data and transmitting the encrypted data; data receivers (3a, 3b, 3c) for receiving the encrypted data from the data transmitter; satellite links (4, 4a) used for data transmission from the data transmitter to the data receivers; and bidirectional communication channels (9) which are also used for transmitting data from the data receivers to the data receivers and which have a smaller capacity of data transmission than the satellite links. The satellite links (4, 4a) are used to transmit encrypted data from the data transmitter to the data receivers.; At least the bidirectional communication channels (9) are used to communicate restrictive data transmission control information between the data transmitter (2) and the data receivers (3).

FIG.6



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04L 9/00

(11) 공개번호 특1999-0088222
(43) 공개일자 1999년12월27일

(21) 출원번호 10-1999-0016936
(22) 출원일자 1999년05월12일
(30) 우선권주장 98-129214 1998년05월12일 일본(JP)
(71) 출원인 소니 가부시끼 가이샤 이데이 노부유끼
일본국 도쿄도 시나가와쿠 키타시나가와 6초메 7반 35고
(72) 발명자 하라가즈히로
일본도쿄도시나가와구기타시나가와6-7-35소니가부시키가이샤내
(74) 대리인 이병호

심사청구 : 없음

(54) 데이터전송제어방법및데이터전송시스템

요약

본 발명에 따른 데이터 전송 시스템은 데이터 송신기로부터 데이터 수신기 또는 수신기들로 안전하고 확실한 데이터 전송을 가능하게 한다. 상기 시스템은 데이터를 암호화하여 암호화된 데이터를 전송하는 데이터 송신기와; 상기 데이터 송신기로부터 상기 암호화된 데이터를 수신하는 데이터 수신기와; 상기 데이터 송신기로부터 상기 데이터 수신기로의 데이터 전송에 사용되는 위성 링크와; 상기 데이터 수신기로부터 상기 데이터 수신기로 데이터를 전송하며 상기 위성 링크보다 더 적은 데이터 전송량을 가지는 양방향 통신 채널을 포함한다. 상기 위성 링크는 상기 데이터 송신기로부터 암호화된 데이터를 데이터 수신기로 전송하는데 사용된다. 적어도 상기 양방향 통신 채널은 상기 데이터 송신기와 데이터 수신기 사이에서 데이터 한정 전송 제어 정보를 주고받는데 사용된다.

대표도

도1

색인어

데이터 전송 제어 방법, 데이터 전송 시스템, 데이터 한정 전송 제어 정보, 암호화 키, 세션 키, IP 라우터, 브리지

명세서

도면의 간단한 설명

도 1은 종래의 데이터 전송 시스템의 통상적인 구조의 개략도.

도 2는 종래의 데이터 전송 시스템에 사용되며 행선(destination) 어드레스를 포함하는 이더넷(Ethernet) 프레임의 데이터 구조의 개략도.

도 3은 종래의 데이터 전송 시스템의 데이터 수신기가 상기 이더넷을 통해 수신한 이더넷 프레임이 상기 수신기 자체의 행선 어드레스를 포함하고 있는지의 여부를 검사하고, 상기 행선 어드레스 검사 다음의 과정을 수행하는 단계를 도시한 흐름도.

도 4는 TS 패킷에 대한 데이터 구조 포맷의 개략도.

도 5는 종래의 데이터 전송 시스템에서의 데이터 송신기 및 데이터 수신기 구조의 개략도.

도 6은 본 발명에 따른 데이터 전송 시스템의 개략도.

도 7a 내지 7g는 데이터 전송 시스템에서 데이터 송신기로부터 데이터 수신기로 전송되는, 다수의 프로토콜에 따라서 캡슐화 데이터의 개략도.

도 8은 데이터 전송 시스템에서 데이터 송신기 및 데이터 수신기의 블록도.

도 9는 데이터 송신기로부터 데이터 수신기로 전송되는 데이터를 암호화하는 세션 키를 갱신하는 단계의 흐름도,

도 10은 섹션 **헤더**의 데이터 구조의 개략도,

도 11은 **MAC** 어드레스들이 세션 키(Ks)의 플래그에 대응하여 설정되는 대응표,

도 12는 데이터 송신기가 데이터를 캡슐화하는 단계의 흐름도,

도 13은 IP 어드레스들이 **MAC** 어드레스들에 대응하여 설정되는 대응표,

도 14는 데이터 수신기가 세션 키(Ks)를 사용하여 수신된 데이터를 암호 해독하는 단계의 흐름도,

도 15는 **MAC** 어드레스들이 세션 키(Ks)에 대응하여 설정되는 대응표,

도 16은 IP 데이터그램(datagram)을 추출하는데 사용된 총 길이 필드를 보유하는 데이터 구조에 대한 암호 해독 개략도,

도 17은 데이터 전송 시스템의 제 1 변형의 개략도,

도 18은 데이터 전송 시스템의 제 2 변형의 개략도,

* 도면의 주요 부분에 대한 부호의 설명 *

1 : 데이터 전송 시스템 2 : 데이터 송신기

3 : 데이터 수신기 4 : 통신 위성

5 : 인터넷 서비스 제공업체 6 : 인터넷

7 : 전용선 8 : 전화선

9 : 양방향 통신 채널

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 데이터 송신기로부터 데이터 수신기로의 데이터 전송 제어를 위한 데이터 전송 제어 방법 및 데이터 전송 시스템에 관한 것으로서, 특히, 데이터 송신기로부터 특정 데이터 수신기로 전송된 데이터의 수신을 제한하는 데이터 전송 제어 방법 및 데이터 전송 시스템에 관한 것이다.

최근, 데이터 송신기가 데이터를 복수의 멀리 떨어져 위치하고 있는 데이터 수신기로 송신하도록 하는 네트워크 타입의 데이터 전송 시스템이 개설되었다. 예를 들면, 위성 텔레비전 방송이 위성 링크를 이용하는 방송 데이터 전송 시스템으로 실행되어 영상 및 음성 정보를 복수의 데이터 수신기에 공급한다.

상기 방송 데이터 전송 시스템의 다른 예로는 로컬 에리어 네트워크(LAN)로서 설정되는 이더넷(Ethernet)이 있다. 도 1에 도시한 바와 같이, 이더넷 네트워크는 통상적으로 데이터를 송신하는 데이터 송신기(351) 및 상기 데이터 송신기(351)로부터 네트워크(353)를 통하여 데이터를 수신하는 데이터 수신기(352a 및 352b)로 구성된다. 이더넷 상의 데이터 수신기들 사이의 최대 허용 거리는 수 킬로미터로 설정되어 있다.

상기 데이터 전송 시스템에서 상기 데이터 송신기(351)가 데이터 수신기(352a)에 데이터를 전송하는 경우, 상기 데이터 송신기(351)는 네트워크(353) 상으로 상기 데이터를 전송한다. 전송된 데이터에는 행선 데이터 수신기(352a)를 식별하는 행선 어드레스가 추가된다. 예를 들면, 대용량의 행선 어드레스 정보를 표현하는데 48 비트가 사용된다.

상기 데이터 송신기(351)에 의해 네트워크(353)로 전송된 데이터는 데이터 수신기(352a 및 352b)에 의해 수신된다. 각 데이터 수신기는 상기 수신된 데이터에 추가된 행선 어드레스를 참조하여 상기 어드레스가 자신의 어드레스인지 확인한다. 상기 이더넷에 의해 사용된 통상적인 프레임 포맷은 도 2에 도시된 바와 같이 구성된다. 이 포맷에서, 행선 어드레스부(401)는 상기 데이터를 수신하는 행선 데이터 수신기의 어드레스를 나타낸다.

만약, 지정된 데이터 수신기가 상기 수신된 어드레스가 자신의 어드레스가 아니라고 판정하면, 상기 수신기는 상기 송신된 데이터를 폐기한다. 즉, 상기 데이터 수신기(352a)가 상기 데이터에 추가된 어드레스가 자신의 어드레스라고 판정하면 상기 송신된 데이터를 받아들이고, 상기 데이터 수신기(352a)가 상기 수신된 데이터에서 자신의 어드레스를 검출하지 못하면 그 데이터를 폐기하는 것이다. 이더넷 상에서의 데이터 수신기에 의한 데이터 수신 과정은 일반적으로 도 3의 흐름도를 구성하는 단계들에서 도시한 바와 같이 진행한다.

단계 S101에서, 상기 데이터 수신기는 로컬 에리어 네트워크로부터 데이터를 포함하는 이더넷 프레임을 수신한다. 단계 S102에서, 상기 데이터 수신기는 상기 수신된 이더넷 프레임으로부터 행선 어드레스를 추출한다. 단계 S103에서, 상기 데이터 수신기는 상기 행선 어드레스가 자신의 어드레스(유니캐스트(unicast) 어드레스)인지 또는 자신이 속한 어드레스(멀티캐스트(multicast) 어드레스)인지 검사한다. 만약 상기 행선 어드레스가 수신기 그 자체의 어드레스(유니캐스트 어드레스) 또는 그것이 속한 어드레스(멀티캐스트 어드레스)인 것으로 판정되면, 상기 데이터 수신기는 상기 이더넷 프레임을 호스트 컴퓨터에 전송한다. 유니캐스트 어드레스는 개별적인 수신기를 지정하는 어드레스를 나타내고, 멀티캐스트 어드레스는 그 어드

레스와 관련하여 전송된 데이터를 수신하는 복수의 데이터 수신기(예를 들면, 데이터 수신기 그룹)를 허용하는 어드레스이다.

만약, 상기 행선 어드레스가 요구된 데이터 수신기를 지정하는 어드레스(유니캐스트 어드레스)도 상기 데이터 수신기가 속한 어드레스(멀티캐스트 어드레스)도 아니라고 판정하면, 상기 데이터 수신기는 상기 이더넷 프레임을 폐기한다.

상기 행선 어드레스 구조에 의거한 데이터 전송 방법에 따르면, 어드레스가 전송된 행선 어드레스와 일치하지 않는 어떠한 데이터 수신기도 그 어드레스로 공급된 데이터를 수신할 수 없을 것이다. 그러나, 사실은 상기 데이터 전송 방법에 의해 데이터 수신기가 자신의 어드레스를 가질 수도 있으며 다른 지정된 데이터 즉, 요구된 데이터 수신가를 나타내는 행선 어드레스가 없는 데이터를 받아들이도록 수정된 판정 특성을 가질 수도 있다. 이러한 가능성은 비밀 데이터가 특정 데이터 수신기에 전송될 필요가 있는 경우에 보안상의 문제를 유발할 것이다.

이더넷 상에서, 동일 네트워크에 접속된 데이터 수신기의 수는 제한되고, 접속된 수신기 사이의 거리도 제한된다. 이것은 하나의 데이터 수신기로 전송된 데이터가 다른 데이터 수신기에 의해 불법으로 연결될 수도 있음을 의미한다. 예를 들면, 10BASE-5의 통상적인 이더넷 구조에서, 한 **세그먼트**에 대한 최대 케이블 길이는 500 미터로 제한되고 네트워크에 접속할 수 있는 트랜시버(데이타 송수신기)의 수는 100까지로 설정된다.

반면에, 데이터 전송 네트워크가 위성 링크를 이용하여 구성되면, 하나의 네트워크는 일본과 같은 한 국가 전체보다 더 넓은 영역을 커버할 수 있다. 이러한 네트워크 상에서, 홋카이도의 최북단 섬에 위치한 데이터 수신기로 전송된 데이터가 최남단의 오키나와 현에 위치한 데이터 수신기에 의해 도청될 수 있다. 즉, 다수의 데이터 수신기로 구성되는 임의의 위성 링크 기준 네트워크 상에서는, 예상치 못한 무리에 의해 불법으로 도청될 가능성이 증가한다.

위성 링크와 같은 방송 타입 통신 채널을 이용한 데이터 전송 설정에서는, 처리되지 않은 데이터가 요청한 데이터 수신기뿐만 아니라 요구한 데이터를 수신하리라 예상치 못한 수신기에 의해서도 수신될 수 있다. 통신 위성을 이용하는 오늘날의 디지털 데이터 방송 시스템에 나타나는 이 문제에 대한 한가지 해결책은 위성 통신 링크를 통하여 데이터를 전송하기 전에 데이터(주로 영상 및 음성 정보)를 암호화하는 것이다. 데이터 수신기들은 원래의 데이터를 재구성하는 암호 해독 기능을 가진다. 이러한 타입의 데이터 전송 시스템에서는, 데이터를 수신하도록 사전에 허가된 데이터 수신기들만 음성-영상물에 대한 전송을 암호 해독할 수 있다. 이러한 시스템 중 한 시스템은 통신 기술 협회(일본)에 의한 보고서 제 74번에 기초한다. 상기 시스템은 전송 포맷으로서 **MPEG2**(동화상 전문가 그룹 제 2단계) 전송 스트림 패킷(TS 패킷)을 이용한다. 예를 들면, 상기 시스템은 암호화 키를 사용하는 데이터를 암호화하는 데이터 송신기를 가지며 상기 암호화 키에 대응하는 암호 해독 키를 사용하는 암호화된 데이터를 해독하는 데이터 수신기를 가진다. 상기 TS 패킷의 포맷은 도 4에 도시되어 있다. 상기 포맷의 **헤더**에 있는 PID(패킷 식별) 부(411) 및 스크램블 제어부(412)는 암호화 키를 판정한다. 일반적으로, 상기 암호화 키는 세션 키(Ks) 및 작업 키(Kw)를 포함한다. 상기 PID 부분(411)은 13 비트의 데이터를 구성하고 상기 스크램블 제어부(412)는 2 비트 데이터를 구성한다.

상기 TS 패킷으로 데이터를 전송하도록 설정된 현재의 위성 텔레비전 방송에서 데이터 전송 시스템은 도 5에 도시되어 있는 바와 같이 데이터 송신기(501) 및 데이터 수신기(511)를 포함한다. 상기 데이터 송신기(501)는 다양한 암호 키를 사용하여 데이터 암호화를 행하는 암호 유닛(502, 503, 504)을 가진다. 상기 데이터 수신기(511)는 다양한 암호 키를 사용하여 데이터 해독을 하는 암호 해독 유닛(512, 513, 514) 및 허가 판단 유닛(515)을 가진다.

상기 구조의 데이터 전송 시스템에서, 상기 데이터 송신기(501)는 먼저 작업키(506)를 상기 데이터 수신기(511)로 전송한다. 특히, 상기 데이터 송신기(501)는 상기 PID 부분(411) 및 스크램블 제어부(412)에 대응하는 작업 키(Kw)(506)를 미리 준비한다. 그 다음에 상기 데이터 송신기(501)는 마스터 키(Km)(507)를 이용하여 암호화 유닛(504)에 의해 암호화된다. 상기 암호 작업키(Kw)(506)는 상기 데이터 수신기(511)로 전송된다. 마스터 키(Km)(507)는 데이터 수신기(511) 고유의 마스터 키(해독키)(Km)(518)와 동일하다. 상기 암호화된 작업키(Kw)(506)는 상기 데이터 송신가(501)로부터 위성 링크를 통하여 데이터 수신기(511)로 전송된다.

상기 마스터 키(Km)(507)로 암호화된 작업키(Kw)(506)를 수신하면, 상기 데이터 수신기(511)는 자체의 마스터 키(Km)(518)를 이용하여 상기 수신된 키를 해독한다. 상기 해독된 작업키(Kw)(517)는 상기 PID 부분에 대응하도록 보존한다. 상기 작업키(Kw)(517)는 상기 데이터 송신기(501)로부터 전송되는 암호화된 데이터를 해독하는데 사용된다.

상기 데이터 송신기(501)로부터 데이터 수신기(511)로의 데이터 전송시, 상기 데이터 송신기(501)는 세션 키(Ks)(505)를 이용하여 상기 암호화 유닛(502)에 의해 암호화된 TS 패킷에 데이터의 **페이로드**부(413)를 가진다. 동시에, 상기 세션 키(Ks)(505)는 상기 작업키(Kw)(506)를 이용하여 상기 암호화 유닛(503)에 의해 암호화된다.

상기 데이터 수신기(511)를 행선으로 식별하는 PID 부분을 갖는 TS 패킷 수신시, 상기 데이터 수신기(511)는 전송된 TS 패킷 내의 PID 부분(411)에 의거하여 사전에 보존된 작업키(Kw)(517)를 추출한다. 상기 데이터 수신기(511)는 상기 추출된 작업키(Kw)(517)를 이용하여 상기 데이터 송신기(501)로부터의 데이터와 함께 전송된 상기 암호화된 세션 키(Ks)(505)를 해독한다. 이렇게 해독된 세션 키(Ks)(516)를 이용하여, 상기 데이터 수신기(511)는 상기 TS 패킷의 상기 **페이로드** 부분(413)을 해독하여 상기 데이터를 추출한다.

상기 작업키(Kw)가 아직 이들 데이터 수신기로 전송되지 않았기 때문에 허가되지 않은 데이터 수신기는 시청하고 싶은 PID 부분에 대응하는 적절한 작업키(Kw)를 가지고 있지 않다. 이러한 데이터 수신기는 상기 데이터 송신기(501)가 상기 작업키(Kw)를 이용한 그 다음 키 암호화에 이어 전송한 상기 세션 키(Ks)를 해독할 수 없다. 해독되지 않은 세션 키(Ks)를 가지고는, 허가되지 않은 데이터 수신기가 데이터 송신기

(501)로부터 상기 암호화된 데이터를 해독할 수 없다. 바꾸어 말하면, 허가되지 않은 데이터 수신기는 암호화된 데이터만 수신할 수 있고 음성 영상물에 대한 데이터를 해독할 수는 없다.

위성 링크를 이용하는 상기 방송 시스템은 전술한 바와 같이 데이터 한정 전송 제어를 행한다. 데이터 한정 전송 제어에 대한 많은 다른 방법들이 방송 시스템 및 인터넷을 통해서 실행되고 있다.

인터넷 상에서는, 전자 메일을 암호화하여 도청 또는 위조를 방지하기 위해 PGP(Pretty Good Privacy) 및 PEM(Privacy Enhanced Mail)을 이용한다. 또한 인터넷 상에서는 HTTP(Hyper Text Transfer Protocol)에 의거한 전자 상거래에서 유통하는 신용카드 번호의 불법 도청을 막기 위해서 SSL(Secure Socket Layer)을 이용한다. 이러한 계획들은 암호화 시스템을 이용하거나 또는 유연한 데이터 전송 제어를 채용하고 있다는 특징이 있다.

IP(Internet Protocol) 데이터그램에 대한 보다 일반화된 데이터 전송 제어 방법이 있다. 이러한 종류의 표준화된 방법들은 AH(Authentication Header) 및 일반적으로 IPSEC라고 하는 ESP(Encapsulating Security Payload)를 포함한다.

위성 링크를 이용하는 텔레비전 방송과 관련하여 다음의 문제점들이 일반적으로 나타나고 있다.

첫 번째 문제점은 허가된 데이터 수신기의 수의 제한이다. 도 4에 도시된 바와 같이, 암호화 키를 식별하는 PID 부분과 스크램블 제어부는 단지 13 비트 및 2비트만을 각각 포함한다. 이것은 15 비트가 2^{15}(=32,768)개 까지의 데이터 수신기를 지정하는데 사용된다는 것을 의미한다.

두 번째 문제점은 사용중인 PID의 수가 증가함에 따라서 송신측에서의 비용이 증가한다는 것이다. 예를 들면, 데이터 수신기는 PID의 수에 거의 비례하는 개수의 MPEG2 인코더를 필요로 한다. 따라서 PID 수가 증가함에 따라서 대규모의 설비를 요하는 데이터 송신측에 비용이 증가되게 된다.

세 번째 문제점은 위성 링크를 통한 일방적인 데이터 송신에서 데이터 송신기는 정보가 행선 데이터 수신기로 정확하게 송신되었는지 알 수 없다는 것이다. 예를 들면, 데이터 송신기를 인식하지 못하면, 데이터 수신기가 허가된 상태임에도 불구하고 실제로는 상기 송신기로부터의 데이터를 수신할 수 없는 경우가 있다는 것이다. 그러나, 정보를 보다 신뢰성 있게 데이터 수신기에 전송하는 방법은 시간이 걸린다. 이것은 많은 자원의 낭비를 초래하며, 이 때문에 유연한 데이터 전송 제어에 대해 장애가 된다.

네 번째 문제점은 IP 데이터그램이 데이터 송신기에 의해 IP 행선 어드레스로 조정된 자체 PID를 가지고 전송되어야 하는 경우, 인터넷 프로토콜과 관련이 적다는 것이다. 특히, IP 데이터그램의 행선 어드레스는 13 비트 PID 부분에 대하여 조정하기 어려운 32 비트 어드레스 포맷을 가진다. 또한, 현재 인터넷 상에서 사용되는 전술한 방법은 다음과 같은 다섯 번째 문제점을 갖는다. 즉, PGP, PEM, SSL은 특정 데이터 전송 제어를 위한 애플리케이션이며 인터넷 상의 모든 애플리케이션에 공통인 것은 아니다. 각 애플리케이션이 자체 제어 방법을 가질 필요가 있기 때문에, 새롭게 도입된 애플리케이션의 신속한 처리가 어렵게 된다.

여섯 번째 문제점은 허가 헤더 및 캡슐화 보안 페이로드가 애플리케이션과 무관하며, 인터넷 프로토콜의 현재 버전(예를 들면, IP v4)의 수준에서 이들 방법과 호환가능한 네트워크 장치들이 사실상 없다는 것이다. 인터넷 프로토콜의 다음 버전(예를 들면, IP v6)은 AH 및 ESP가 규격화된 형태로 인터넷 상에서 사용되도록 허용하고 있지만, 이들은 현재의 인터넷 상에서 실질적으로는 사용불가능한 것으로 생각된다.

발명이 이루고자 하는 기술적 과제

본 발명은 데이터 송신기로부터 데이터 수신기로의 데이터 전송에 있어서, 보다 더 안전하고 확실한 데이터 전송 제어 방법 및 데이터 전송 시스템을 제공한다.

본 발명의 일실시예에 따르면, 상기 데이터 송신 수단에 의해 암호화된 데이터를 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 데이터 전송을 위해 제공된 제 1 통신 채널을 통해 상기 데이터 수신 수단으로 전송하는 단계와, 상기 암호화된 데이터가 적어도, 상기 제 1 통신 채널보다 더 적은 데이터 전송량을 가지며 또한 상기 데이터 수신 수단으로부터 상기 데이터 송신 수단으로의 데이터 전송에 사용되는 제 2 통신 채널을 통해, 특정 데이터 수신 수단에 의해서만 수신되도록 데이터 한정 전송 제어 정보를 상기 데이터 수신 수단으로 전송하는 단계를 포함하는 데이터 전송 제어 방법이 제공된다.

상기 데이터 전송 제어 방법에 의하면, 상기 데이터 송신 수단은 제 1 통신 채널을 통하여 상기 데이터 수신 수단으로 데이터를 전송한다. 데이터 한정 전송 제어 정보는 상기 데이터 송신 수단과 데이터 수신 수단 사이의 적어도 제 2 통신 채널을 통하여 교환될 수도 있다. 상기 제 2 통신 채널을 통하여, 상기 데이터 송신 수단과 특정 데이터 수신 수단 사이의 데이터 교환에 대한 정보가 이들 사이에서 전송될 수도 있다.

예를 들면, 본 발명의 방법에 의하면, 상기 데이터 송신 수단은 특정 데이터 수신 수단으로 송신된 데이터가 정확하게 수신되었는지 알 수 있다.

본 발명의 다른 실시예에 따르면, 데이터 송신 수단으로부터 데이터 수신 수단으로의 데이터 전송에 사용된 제 1 통신 채널과; 상기 데이터 송신 수단과 상기 데이터 수신 수단 사이의 양방향 통신을 가능하게 하는 제 2 통신 채널을 포함하고; 상기 제 1 통신 채널은 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로 암호화된 데이터를 전송하는데 사용되고; 적어도 상기 제 2 통신 채널은 상기 암호화된 데이터가 특정 데이터 수신 수단에 의해서만 수신되도록 데이터 한정 전송 제어 정보를 전송하는데 사용되는 데이터 전송 시스템이 제공된다.

상기 구조의 데이터 전송 시스템에서, 상기 데이터 송신 수단은 제 1 통신 채널을 통하여 상기 데이터 수신 수단으로 데이터를 전송한다. 데이터 한정 전송 제어 정보는 상기 데이터 송신 수단과 상기 데이터 수

신 수단 사이의 제 2 통신 채널을 통하여 교환되고, 상기 제 2 통신 채널은 적어도 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 데이터 전송에 사용되며, 상기 제 1 통신 채널보다 더 적은 데이터 전송량을 가진다.

상기 본 발명의 데이터 전송 시스템에서, 상기 데이터 송신 수단은 데이터 한정 전송 제어 정보를 포함하는 데이터를 제 1 및 제 2 통신 채널을 통하여 데이터 수신 수단으로 전송할 수도 있다. 상기 제 2 통신 채널 상에서, 데이터 송신 수단과 특정 데이터 수신 수단 사이의 데이터 교환에 대한 정보는 이들 사이에서 전송될 수도 있다.

예를 들어 상기 본 발명의 시스템에 의하면, 데이터 송신 수단은 특정 데이터 수신 수단으로 송신된 정보가 정확히 수신되었는지 알 수 있다.

본 발명의 다른 특징에 의하면, 복수의 프로토콜에 따라서 데이터 송신 수단으로부터 데이터 수신 수단으로 전송되는 데이터를 멀티플렉스된 형태로 전송되도록 캡슐화하는 단계와; 상기 캡슐화에 의한 데이터 캡슐들 중 적어도 하나를 암호화하는 단계를 포함하는 데이터 전송 제어 방법이 제공된다.

상기 데이터 전송 제어 방법을 이용하면, 데이터 송신 수단으로부터 데이터 수신 수단으로 전송되는 데이터가 복수의 프로토콜에 맞추어 멀티플렉스된 형태로 캡슐화된다.

상기 본 발명의 방법에 의하면, 관련 프로토콜 요청과 함께 전송되는 데이터가 그대로 유지된다. 이것은 데이터가 특정 프로토콜과 호환성을 가지면서 전송될 수도 있다는 것을 의미한다. 요구된 데이터를 기억하기 위한 공간을 확보하기 위해 프로토콜에 맞추어 데이터가 캡슐화되는 경우, 다양한 종류의 정보를 수용하는 데이터 공간이 제공된다. 상기 캡슐화된 데이터를 암호화하면 한층 더 안전해진다.

예를 들면, 특정 데이터를 수용할 수 있는 프로토콜에 따라서 데이터가 캡슐화될 수도 있다. 상기 캡슐화 과정은 핸션 어드레스에 대한 암호화 키와 같은 정보를 기억할 수 있는 공간을 제공한다. 상기 핸션 어드레스 정보는 어드레스 정보가 PID 부분 및 스크램블 제어부에 기록되는 종래의 TS 패킷 구조에 비해서 상당히 증가된다. 따라서 상기 PID 부분을 확장할 필요가 없어진다.

또한, 각각의 애플리케이션이 자체 제어 방법을 구비할 필요가 없게된다. 이것은 새롭게 도입된 애플리케이션이 본 발명에 의해 신속히 처리될 수 있음을 의미한다. 또한, 허가 **헤더**(AH) 및 캡슐화 보안 **페이로드**(ESP)가 현재의 인터넷 상에서 사용될 수 있다.

본 발명의 다른 특징에 따르면, 암호화 키를 사용하여 데이터를 암호화하는 단계와; 상기 암호화된 데이터에 요구된 데이터를 암호화하는데 사용된 상기 암호화 키에 대한 암호화 키 정보를 부가하는 단계와; 상기 암호화 키 정보와 함께 상기 암호화된 데이터를 데이터 송신 수단으로부터 데이터 수신 수단으로 전송하는 단계와; 상기 데이터 수신 수단이 상기 암호화된 데이터를 해독하도록 하고 자주 갱신되는 복수의 암호 해독 키 중 하나의 해독 키를 이용하여 상기 암호화된 데이터를 해독하고, 상기 하나의 암호 해독 키는 상기 암호화된 정보에 부가된 상기 암호화 키 정보에 따라서 선택되는 데이터 전송 제어 방법이 제공된다.

상기 방법에 따르면, 암호화 키를 이용하여 데이터 암호화 단계에서 암호화된 데이터는 요구된 데이터를 암호화하는데 사용된 상기 암호화 키에 대한 암호화 키 정보를 갖는다. 상기 데이터 전송 단계에서, 상기 암호화된 데이터는 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로 암호화 키 정보와 함께 전송된다. 상기 데이터 해독 단계에서, 상기 암호화된 데이터는 상기 데이터 수신 수단이 상기 암호화된 데이터를 해독하도록 하고 자주 갱신되는 복수의 해독 키들 중 하나의 키를 이용하여 해독되고, 상기 해독 키들 중 하나의 키는 상기 암호화된 데이터에 부가된 암호화 키 정보에 따라서 선택된다.

상기 데이터 전송 제어 방법에 의해, 상기 데이터 송신 수단은 암호화 키를 사용하여 데이터를 암호화한다. 상기 데이터 수신 수단은 자주 갱신되는 복수의 해독 키들 중 한 키를 이용하여 수신된 상기 암호화된 데이터를 해독한다. 상기 하나의 해독 키는 상기 암호화된 데이터와 함께 전송된 암호화 키에 의거하여 상기 데이터 수신 수단에 의해 복수의 암호화 키들 가운데서 선택된다.

본 발명의 다른 목적, 특징 및 이점은 첨부된 도면을 참조하여 보다 명확히 설명한다.

발명의 구성 및 작용

이하, 첨부한 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 본 발명을 구현하는 하기의 데이터 전송 시스템은 데이터 송신기에 의해 위성 링크를 통해 전송된 데이터의 수신을 특정 데이터 수신기로 한정하는 시스템이다.

도 6에 도시된 바와 같이, 본 발명의 데이터 전송 시스템은 데이터 송신기(2)로부터 위성 링크(4a), 통신 채널 역할을 하는 전용선(7) 및 전화선(8), 양방향 통신 채널(9)을 통하여 데이터 수신기(3a, 3b, 3c)로의 데이터 전송을 제어한다. 상기 시스템에서, 상기 데이터 송신기(2)는 데이터를 암호화하여 이 암호화된 데이터를 상기 통신 채널들을 통해 데이터 수신기(3a, 3b, 3c)로 전송한다.

상기 데이터 전송 시스템(1)은 통신 위성(4)을 이용하여 상기 데이터 송신기(2)가 데이터를 데이터 수신기(3a, 3b, 3c)로 송신하도록 하는 통신 채널(4a)과, 전용선(7), 전화선(8) 및 상기 데이터 송신기(2)와 상기 데이터 수신기(3a, 3b, 3c) 사이에서 양방향 통신을 하는 제 2 통신 채널 역할을 하는 양방향 통신 채널(9)을 포함한다. 데이터 전송 시스템(1)은 상기 데이터 송신기(2)로부터 데이터 수신기(3a, 3b, 3c)로 암호화된 데이터를 전송하기 위한 제 1 통신 채널을 사용하며, 데이터 송신기로부터 데이터 수신기로 데이터 한정 전송 제어 정보를 전송하기 위한 제 2 통신 채널을 채용한다. 상기 데이터 전송 시스템(1)은 인터넷에 접속된다.

상기 데이터 한정 전송 제어 정보는 특정 데이터 수신기 또는 수신기들이 상기 데이터 송신기(2)로부터 송신된 데이터를 수신하도록 한다. 바꾸어 말하면, 상기 데이터 한정 전송 제어 정보는 특정 데이터 수신기

또는 수신기들이 소정의 전송된 데이터를 수신하도록 허가한다.

전술한 통신 채널을 이용하여, 데이터 송신기(2)는 다양한 데이터를 데이터 수신기(3a, 3b, 3c)로 전송한다. 상기 데이터 수신기(3a, 3b, 3c)는 통신 채널을 통해 들어오는 데이터를 수신한다. 도 6에서는 단지 세 개의 데이터 수신기(3a, 3b, 3c)만 도시하였지만, 상기 데이터 전송 시스템(1)은 실제로는 수백 내지 수십만개의 데이터 수신기를 포함할 수도 있다.

다음은 데이터 송신기(2)와 데이터 수신기(3a, 3b, 3c)(이하, 각각의 데이터 수신기(3a, 3b, 3c)를 서로 구별할 필요가 없으면 데이터 수신기(3)이라 한다) 사이의 데이터 교환을 허용하는 통신 채널에 대하여 설명한다.

위성 링크(4a)는 대역폭이 약 30Mbps인 Ku 대역 상의 일방향 회로이다. 상기 위성 링크(4a)는 상기 데이터 송신기(2)가 데이터를 예를 들어, 일본 전역에 걸쳐있는 데이터 송신기로 동시에 전송하도록 한다.

상기 양방향 통신 채널(9)은 데이터 송신기(2)와 데이터 수신기(3) 사이에 위성 링크(4a)와 무관하게 설치된다. 이들의 이름이 암시하는 바와 같이, 상기 양방향 통신 채널(9)은 데이터 송신기(2)와 데이터 수신기(3) 사이에 양방향 통신을 가능하게 한다. 따라서, 상기 양방향 통신 채널(9)은 이하 인터넷 상에서의 통신에 사용하기 위한 범용 통신 채널이라고 가정한다.

전용선(7)은 상기 데이터 송신기(2)를 데이터 수신기(3)와 직접 연결하는 통신 수단이다.

인터넷(6)은 영상 및 음성 정보와 같은 다른 종류의 정보를 제공한다. 인터넷 서비스 제공업체(5)는 상기 데이터 수신기(3)를 인터넷과 교통하도록 한다. 데이터 송신기(2)는 인터넷(6)에 접속된다고 가정한다.

전용선(7), 전화선(8), 데이터 송신기(2)와 데이터 수신기(3) 사이의 데이터 교환을 가능하게 하는 양방향 통신 채널(9)은 위성 링크(4a)보다 더 작은 대역 용량을 가진다. 일반적으로, 상기 라인(7, 8, 9)은 수 Kbps로부터 수백 Kbps에 달하는 대역폭을 제공한다.

데이터 전송 시스템(1)은 또한 단지 특정 데이터 수신기 또는 수신기들만 소정의 데이터를 수신하도록 하는 데이터 한정 수신 시스템으로 구성된다. 따라서, 상기 데이터 전송 시스템(1)은 데이터를 예를 들어, 데이터 수신기(3a)로만(유니캐스트형 데이터 공급) 전송하거나 데이터 수신기(3a 및 3b) 그룹(멀티캐스트 데이터형 공급)으로만 전송하거나 또는 모든 수신기들(3a, 3b, 3c)(방송 데이터형 공급)로 전송할 수 있다.

데이터 전송 시스템(1)에서, 데이터 송신기(2)는 데이터를 다음과 같이 데이터 수신기(3)로 송신한다. 즉, 데이터 송신기(2)로부터 데이터 수신기(3)로 전송될 데이터는 도 7a 내지 7g에 도시된 바와 같이 캡슐화된다. 캡슐화는 소정 데이터를 전송하는 데이터 송신기(2)에 의해 행해진다. 제 1 캡슐화 단계에서, 데이터 수신기(3)로 송신될 상기 데이터는 제 1 프로토콜에 따라서 캡슐화된다. 제 2 캡슐화단계에서, 상기 제 1 프로토콜에서 캡슐화된 데이터는 제 2 프로토콜에 따라서 또한 캡슐화된다. 상기 캡슐화 공정은 처리되지 않은 데이터를 소정의 통신 프로토콜에 의해 규정된 전송 포맷에 의거하여 형성된 캡슐(즉, 패킷 또는 프레임)로 주입하는 공정을 포함한다. 데이터를 이러한 캡슐들에 배치하므로서, 이들의 전송 제어가 가능하게 된다.

제 1 캡슐화 단계에서, 데이터 수신기(3)로 송신될 전체 타겟 데이터를 요구된 실제 데이터부와 관련된 부가적인 정보부를 갖춘 실제 데이터부로 배치하므로서 캡슐이 형성된다. 상기 캡슐내 실제 데이터는 암호화된다. 이하 상기 제 1 캡슐화 단계를 보다 상세히 설명한다.

IP(인터넷 프로토콜) 데이터그램(101)은 도 7a에 도시된 바와 같이 인터넷 프로토콜에 의거한 데이터로 구성된다. 상기 **IP** 데이터그램(101)의 데이터는 데이터 송신기(3)로 전송된다. **IP** 데이터그램의 **헤더**는 예를 들면, 인터넷 상의 상기 데이터그램의 행선을 나타내는 행선 어드레스를 포함한다.

상기 **IP** 데이터그램(101)은 인터넷 프로토콜에 의거하여서만 구성되는 것은 아니며, 이더넷 프로토콜에 따라서 구성될 수도 있다.

도 7b 내지 7d에서, 데이터 송신기(2)는 전술한 제 1 프로토콜에 따라서 상기 데이터를 캡슐화한다. 예를 들면, DVB(Digital Video Broadcasting)를 위한 멀티 프로토콜 캡슐화가 제 1 프로토콜로 채용될 수도 있다.

도 7b에 도시된 바와 같이, 상기 데이터 송신기(2)는 먼저 **IP** 데이터그램을 삽입하므로서(즉, 패딩부(102)를 추가) 제 1 프로토콜에 따라서 데이터 캡슐화를 행하여 상기 데이터부의 길이를 64 비트의 정수배로 한다. 예를 들면, 0 내지 63 비트의 패딩부가 상기 IP 데이터그램에 추가된다. 상기 패딩은, 데이터부의 길이가 64 비트의 정수배인 경우에 상기 데이터부가 캡슐화에 적합하기 때문에, 상기 데이터그램을 소정의 데이터 길이로 유지하기 위한 것이다. 상기 제 1 프로토콜의 포맷에 위치한 데이터부는 이하 섹션이라 한다.

상기 패딩(102)으로 추가된 섹션은 도 7c에 도시된 바와 같이 데이터 송신기(2)에 의해 암호화된다. 암호화는 암호화 키를 이용하여 행해진다. 상기 암호화 키는 데이터 수신기(3)로 전송될 정보를 암호화하는데 사용되는 세션 키(하기에 설명됨)이다. 여기서 사용된 상기 암호화 방법은 트리플 DES와 같은 공통키 암호법에 의거한 블록 암호화 방법이다. 상기 트리플 DES 암호화는 현재 가장 강력한 공용키 암호법들 중 하나로서, 하드웨어 상에서 고속 암호화를 수행하기 쉽다. 상기 암호화 공정은 대부분의 공용키 암호법의 공정과는 달리, 30 Mbps 정도의 고속 전송률을 갖는다.

도 7d에 나타낸 바와 같이, 상기 데이터 송신기(2)는 암호화된 섹션 데이터부(104)에 섹션 **헤더**(103) 및 에러 검출을 위한 테일러(105)를 부가한다.

상기 암호화된 섹션 데이터부(104)는 **MAC**(Media Access Control) 프레임 구조를 채용한다. **MAC** 프레임 구성 공정에서, **MAC 헤더**가 상기 데이터부에 부가된다. 상기 **MAC 헤더**를 참조하면 상기 프레임 내에 위치된 데이터의 행선에 대한 제어를 용이하게 할 수 있다. 특히, 상기 **MAC** 프레임은 상기 프레임내에 기억된

데이터를 수신하도록 허가된 데이터 수신기의 행선 어드레스를 수용한다.

상기 섹션 **헤더**(103)는 48 비트 행선 어드레스를 수용할 수 있는 데이터 공간을 제공한다. 특히, 상기 섹션 **헤더**(103)는 상기 행선 어드레스를 포함하도록 형성된 **MAC 헤더**를 가진다. 상기 섹션 **헤더**(103) 내에 48 비트의 행선 어드레스를 수용하는 데이터 공간을 제공하면, 전술한 첫 번째 문제점, 즉, 데이터 수신기의 수적 제한 문제를 해결할 수 있다. 왜냐하면, 확장 어드레스 공간이 암호화 키를 식별하는 많은 정보를 수용하기 때문이다. 또한, 인터넷 프로토콜과의 약한 관련성에 대한 전술한 네 번째 문제점을 해결할 수 있다. 왜냐하면, 데이터그램 전송시에 **IP** 행선 어드레스에 대한 **IP** 데이터그램(101)의 패킷 ID(하기에 설명됨)를 조정할 필요가 없기 때문이다.

상기 테일러(105)는 CRC(Cyclic Redundancy Checking)에 따라 부호화된다. CRC는 **MAC** 프레임 내에 데이터를 수신하는 데이터 수신기(3)가 프레임이 위성 링크를 통해 정상적으로 전송되었는지를 확인하도록 설계된다. 예를 들면, CRC는 32비트로 부호화되어 있다.

지금까지 제 1 프로토콜에 따라서 전송될 데이터를 캡슐화하는 것에 대해 설명하였다. 다음은 상기 제 1 프로토콜에 따라서 캡슐화된 데이터가 제 2 크로토콜에 따라서 캡슐화되는 방법에 대하여 설명한다.

제 2 프로토콜에 의거한 데이터 캡슐화는 복수의 패킷을 상기 제 1 프로토콜에 따라서 캡슐화된 데이터로 분할하는 단계를 포함한다. 상기 제 2 프로토콜은 데이터의 캡슐화를 **MPEG2**(Moving Picture Experts Group Phase 2)에 의거한 TS(Transport Stream) 패킷들로 규정하는 프로토콜이다. 상기 TS 패킷들은 음성 및 영상 신호들 및 다른 데이터와 같은 많은 종류의 데이터가 멀티플렉스되어 대용량 디지털 라인들을 통해 전송되도록 한다. 제 2 프로토콜에 따르면, 상기 데이터는 도 7e 내지 7g에 도시한 바와 같이 복수의 TS 패킷(106, 107, 108)으로 캡슐화된다. 상기 TS 패킷들(106, 107, 108)은 각각 TS **헤더**(HTS) 및 TS **페이로드**부(P)로 구성된다. 상기 TS **페이로드**부(P)는 제 1 프로토콜에 따라서 분할되어 캡슐화된 데이터를 포함한다. 각 TS 패킷의 TS **헤더**(HTS)는 도 4에 도시된 바와 같이 패킷 ID(PID) 부분과 스크램블 제어부로 구성된다. 통상적으로, 행선 어드레스는 PID 부분 및 스크램블 제어부에 기록된다는 사실이 행선 어드레스 정보의 범위를 한정하였다. 본 실시예에서는 행선 어드레스가 섹션 **헤더**(103)에 기록되기 때문에 상기 문제점이 해소된다.

이상 제 2 프로토콜에 따른 데이터 캡슐화를 설명하였다. 전술한 바와 같이, 상기 데이터 송신기(2)는 데이터를 캡슐화하여 제 1 및 제 2 프로토콜에 따라서 멀티플렉스된 형태로 데이터 수신기(3)(**IP** 데이터그램)로 송신한다. 상기 캡슐화된 데이터는 통신 위성(4)으로 진행한다.

데이터 한정 전송 제어는 두 레벨, 즉, TS 패킷 레벨 및 섹션 레벨에서 개별적으로 이루어지기 때문에, 전술한 두 번째, 다섯 번째 및 여섯 번째 문제점이 해결된다.

특히, 두 번째 문제점, 즉, 사용중인 PID의 수가 증가함에 따른 전송 비용 증대의 문제점을 회피하면서, 다수의 정보를가 암호화 키에 대해서 확보될 수 있다.

다섯 번째 문제점, 즉, 각 애플리케이션이 스스로의 제어 방법을 가져야 하는 문제점이 더 이상 적용되지 않는다. 새롭게 도입된 애플리케이션은 본 실시예에 의해 신속히 처리된다.

상기 여섯 번째 문제점도 또한 본 실시예에 의해 해결된다. 즉, 허가 **헤더**(AH) 및 캡슐화 보안 **페이로드**(ESP)를 현재의 인터넷 상에서 사용할 수 있다.

전술한 **IP** 데이터그램의 캡슐화는 데이터그램이 위성 링크(4a)를 통해 데이터 수신기(3)로 전송될 때 행해진다. 양방향 통신 채널(9)을 통해, 특수한 캡슐화없이 통상의 인터넷이 **IP** 데이터그램을 전송하는데 사용된다.

다음은 암호화 키를 이용하여 데이터가 데이터 송신기(2)에 의해 암호화되는 방법과, 암호화키를 이용하여 (해독키를 이용하여) 데이터 수신기에 의해 상기 암호화된 데이터가 해독되는 방법을 설명한다. 도 8에 도시된 바와 같이 구성된 데이터 송신기(2) 및 데이터 수신기(3)는 도 6에 도시된 통신 채널을 통해 상호 접속된다. 상기 데이터 송신기(2)는 제 1 프로토콜(섹션)에 따라서 데이터를 상기 데이터 수신기(3)로 전송한다. 제 2 프로토콜(TS 패킷)에 따른 데이터 전송은 위에서 도 5의 종래의 구성을 참조하며 설명하였다. 도 8의 본 발명의 장치와 도 5의 종래의 장치를 비교하여 보면, 상기 실시예는 데이터 송신기 및 데이터 수신기에 의한 암호화 및 해독을 위해 두 개의 키 레벨, 즉, 세션 키(Ks)(24) 및 마스터 키(Km)(25) 상에서 동작하는 반면에, 종래의 장치는 세 개의 키 레벨 구조로 되어 있다. 본 실시예에 의하면 하나의 키 레벨을 절감할 수 있다.

상기 세션 키(Ks)(24)는 공통키 암호 시스템 하에서 데이터 암호화 및 해독을 위한 데이터 송신기(2) 및 수신기(3)에 포함된다. 편의를 위해, 데이터 수신기(3)에 포함된 세션 키(Ks)는 하기에 세션 키(Ks)(34)라 지칭한다.

세션 키(Ks)(24)를 사용하면, 상기 데이터 송신기(2)는 특정 데이터 수신기 또는 수신기들로 송신될 데이터를 암호화한다. 상기 데이터 수신기(3)는 세션 키(Ks)(34)를 이용하여 암호화된 데이터를 해독하고, 이에 따라 상기 해독된 데이터로부터 소정의 정보를 추출한다.

세션 키(Ks)(24 및 34)는 규칙적인 간격, 예를 들면, 매일, 매시간 또는 매분마다 갱신된다. 도청자들이 소정 시간에 세션 키(Ks)(24)를 알게되더라도, 이들은 그 데이터를 상기 키에 의해 허가된 제한된 시간 동안만 도청할 수 있다. 세션 키들을 갱신하는 것에 대해서는 하기에 보다 상세히 설명한다.

상기 세션 키(Ks)(24)는 전술한 트리플 DES에 따라서 도 7c에 도시된 섹션 데이터부를 암호화하는데 사용된다.

상기 섹션 키(Ks)(24)와 같이, 마스터 키(Km)(25)는 데이터 송신기(2) 및 데이터 수신기(3) 모두에 포함된다. 각각의 데이터 수신기(3A, 3B, 3C)는 하나의 마스터 키에 할당된다. 편의상, 데이터 수신기(3)에 포함된 상기 마스터 키(Km)는 이하 마스터 키(Km)(35)라 지칭한다.

상기 마스터 키(Ks)(25)는 데이터 송신기(2)와 데이터 수신기(3) 사이에서 전송되지 않는다. 어떠한 마스

터 키도 상기 통신 채널 상에 제공되는 경우는 없다. 상기 마스터 키는 그 사용자를 제외하고는 어떠한 수단에 의해서도 누구도 알 수 없다.

상기 마스터 키(Km)는 상기 세션 키(Ks)를 데이터 수신기(3)로 전송하기 전에 암호화하기 위해 데이터 송신기(2)에 의해 사용되고, 수신된 상기 암호화된 세션 키(Ks)를 해독하기 위해 데이터 수신기에 의해 사용된다. 특히, 상기 데이터 송신기(2)는 상기 마스터 키(Km)(25)를 이용하여 상기 세션 키(Ks)(24)를 암호화하고, 암호화된 세션 키(Ks)(24)를 상기 데이터 수신기(3)로 미리 전송한다. 상기 암호화된 세션 키(Ks)(24)를 수신하면, 상기 데이터 수신기(3)는 마스터 키(Km)를 이용하여 (세션 키(Ks)(34)를 추출하기 위해) 수신된 키를 해독한다.

그 다음에 상기 세션 키(Ks)는 상기 마스터 키(Km)에 의거하여 암호화 및 해독을 거치며, 데이터 송신기(2)로부터 데이터 수신기(3)로의 전송 과정 동안 도청자들에 의한 도청으로부터 보호된다.

상기 해독된 세션 키(Ks)를 이용하여, 상기 데이터 수신기(3)는 요구된 세션 키(Ks)를 사용하여 암호화된 상기 전송된 데이터를 해독한다. 데이터 수신기(3)는 상기 해독된 데이터로부터 의미있는 정보를 추출한다.

상기 세션 키(Ks)는 트리플 DES에 따라서 상기 마스터 키(Km)를 이용하여 암호화되고 해독된다. 대안적으로, 공용 암호 시스템이 채용될 수도 있다. 상기 대안적인 시스템은 데이터의 암호화 및 해독 처리와는 다른 상기 시스템에 의한 키들이 고속으로 수행될 필요가 없으며 이들이 또한 보안을 보장한다는 점에 있어서 이점을 가진다.

상기 세션 키(Ks)(24)와는 달리 상기 마스터 키(Km)(25)는 시간에 따라서 갱신되지 않는다.

이하, 상기 세션 키(Ks)(24)가 갱신되는 방법을 설명한다. 상기 세션 키(Ks)(24)를 갱신하는데 있어서는 데이터 송신기(2)가 능동적으로 사용된다. 상기 마스터 키(Km)(25)를 이용하여 암호화된 세션 키(Ks)(24)(하기에는 암호화된 세션 키(Km(Ks))라 함)는 또한 데이터 송신기(2)에 의해 능동적으로 전송된다.

양방향 통신 채널(9)을 이용하면, 상기 데이터 수신기(3)는 상기 세션 키(Ks)를 능동적으로 요구할 수 있다. 이런 방식으로, 각각의 데이터 수신기(3a, 3b, 3c)는 상기 데이터 송신기(3)로부터 빠르고 확실하게 필요한 세션 키들을 획득할 수 있다. 예를 들면, 새로운 데이터 수신기(3)가 상기 데이터 송신 시스템(1)에 부가되는 경우, 장해에 의해 서비스를 받을 수 없는 데이터 수신기(3)가 장해로부터 회복되어 상기 시스템(1)에 부가되는 경우, 또는 데이터 수신기(3)가 상기 세션 키(Ks)를 정확히 수신하지 못하는 경우, 데이터 수신기에 의해 상기 키에 대한 능동적인 요구를 통하여 빠르고 확실한 세션 키(Ks)(24) 획득이 가능하다. 장해로부터의 회복 및 세션 키(Ks)의 갱신은 데이터 송신기(2) 및 데이터 수신기(3)에 각각 결합된 CA(Conditional Access) 관리 유닛(23 및 33)에 의해 관리된다. 상기 두 유닛(23 및 33)은 서로 교통하여 이들간에 제어 정보를 교환한다.

상기 특징에 의해, 전술한 세 번째 문제점, 즉, 통신 채널로서 위성 링크에만 의존하는 데이터 전송 시스템에서, 정보가 정확히 행선 데이터 수신기로 전송되었는지를 데이터 송신기가 알 수 없다는 문제점을 극복할 수 있다.

상기 데이터 송신기(2)는 세션 키(Ks)를 일방향 위성 링크(4a) 또는 양방향 통신 채널(9)을 통해 데이터 수신기(3)로 전송할 수도 있다.

상기 세션 키(Ks)는 도 9에 도시된 흐름도를 구성하는 단계에서 갱신된다.

소정 시간에서, 상기 데이터 수신기(3)는 두 개의 세션 키(Ks)(34), 즉, 세션 키(Ks_even) 및 세션 키(Ks_odd)를 갖는다. 상기 데이터 수신기(3)는 상기 데이터 송신기(2)로부터 송신된 정보 및 데이터를 해독하는데 두 개의 세션 키들(Ks_even 및 Ks_odd) 중 하나의 키를 사용한다.

현재 사용되고 있는 상기 두 개의 세션 키들(Ks) 중 어느 하나는 도 7d에 도시된 섹션 **헤더**(103)에 가록된 정보에 의해 식별된다. 예를 들면, 도 10에 도시된 바와 같이, 상기 섹션 **헤더**(103)는 표 ID(table_id), **MAC** 어드레스부(**MAC**_address_1, **MAC**_address_2, **MAC**_address_3, **MAC**_address_4, **MAC**_address_5, **MAC**_address_6), 섹션 정보부(section_length, section_number, last_section_number), ssi(section_syntax_indicator), pi(private_indicator), rsvd(reserved), psc(payload_scramble_indicator)(111), asc(address_scramble_indicator), LSf(LLC_SNAP_flag), cni(current_next_indicator)을 포함한다. 상기 psc(111)는 두 개의 세션 키(Ks) 중 어느 키가 현재 사용중인지를 나타낸다. 상기 psc(111)는 2 비트 정보로 이루어진다. 만약 상기 psc의 상위 비트가 "0"이면, 이것은 상기 세션 키(Ks_even)가 사용됨을 의미하고, 만약 상기 psc의 상위 비트가 "1"이면, 이것은 상기 세션 키(Ks_odd)가 현재 사용중임을 의미한다.

도 9의 단계 S1에서, 상기 세션 키(Ks) 중 어느 키가 현재 사용되는지 검사된다. 단계 S2에서, 상기 데이터 수신기(3)는 타이머에 의해 트리거되어 세션 키 갱신 처리를 개시한다.

단계 S3에서, 데이터 수신기(3)는 **MAC** 어드레스가 세션 키(Ks)와 대응하여 포함되어 있는 대응표에서 찾아낸 현제의 세션 키(Ks)의 플래그를 갱신한다. 상기 데이터 수신기(3)는 도 11에 도시되어 있는 바와 같은 **MAC** 어드레스와 세션 키 대응표를 갖는다. 현재 사용된 세션 키(Ks) 내의 플래그는 상기 표에 대하여 갱신된다. 상기 갱신 동작은 상기 psc(111)의 상위 비트를 "0"으로 반전시킨다.

단계 S4에서, 상기 데이터 수신기(3)는 psc(111)에 의거하여 상기 섹션에 포함된 IP 데이터그램을 해독한다. 특히, 상기 psc 상위 비트가 "0"으로 설정되면, 데이터 수신기(3)는 현재의 세션 키(Ks_odd)(psc의 상위 비트가 "1"인 경우에 사용됨)의 사용을 중지하고, 암호 해독을 위해 세션 키(Ks_even)로 전환한다. 상기 psc의 상위 비트가 "1"로 설정되면, 상기 데이터 수신기(3)는 현재의 세션 키(Ks_even)(상기 psc 상위 비트가 "0"인 경우에 사용됨)의 이용을 중단하고 암호 해독을 위해 세션 키(Ks_odd)로 전환한다. 단계 S5에서 세션 키(Ks)가 새로 변경되기 전에, 상기 데이터 송신기(2)는 상기 마스터 키(Km)(24)를 이용하여

다음 세션 키(Ks)를 암호화하여 상기 암호화된 키를 데이터 수신기(3)로 전송한다.

상기 암호화된 세션 키(Km)(Ks)는 위성 링크(4a) 또는 양방향 통신 채널(9)을 통해 송신된다. 송신에 이용된 프로토콜은 TCP/IP(Trasmission Control Protocol/Internet Protocol)와 같은 승인(acknowledgments)을 필요로하는 프로토콜일 수 있다. 상기 프로토콜에 의해 상기 세션 키(Ks)는 데이터 송신기(2)로부터 상기 데이터 수신기(3)로 확실히 전송될 수 있다.

단계 S6에서 상기 세션 키 전송이 행해지고 있는 동안, 상기 데이터 수신기(3)는 도 11에 도시된 **MAC** 어드레스와 세션 키 대응표를 갱신한다. 즉, 현재 사용된 세션 키(Ks)는 다음 세션 키(Ks)로 치환된다.

단계 S7에서, 데이터 수신기(3)는 다음 세션 키(Ks)가 현재 데이터 수신기(3)에 포함되어 있는지 확인한다. 단계 S8에서, 데이터 수신기(3)는 다음 세션 키(Ks)로 전환한다. 단계 S8 내지 S13은 상기 psc의 상위 비트가 "1"로 설정되어 세션 키(Ks_odd)가 암호 해독에 사용되는 과정을 나타낸다. 상기 과정은 단계 S7로부터 시작된 단계이며, 데이터 수신기(3)가 현재의 세션 키(Ks)를 세션 키(Ks_even)(psc의 상위 비트: 0)라고 판단하면 단계 S1로부터 시작되는 단계이다.

상기 단계들을 수행하므로서, 상기 데이터 송신기(2)는 상기 데이터 수신기(3)에 확실하게 갱신되는 세션 키(Ks)를 제공한다. 데이터 수신기(3)는 두 개의 세션 키(Ks)를 동시에 전환하므로 현재 유효한 세션 키(Ks)에 의거한 데이터 해독이 중지되지 않는다. 상기 세션 키(Ks)(24)의 갱신 주파수는 전송 처리 기간에 따라서 유연하게 변할 수도 있다. 상기 세션 키(Ks)는 전술한 바와 같이 데이터 수신기 내에서 규칙적으로 갱신된다. 이렇게 갱신된 세션 키(Ks)를 사용하며, 상기 데이터 수신기(3)는 상기 키와 함께 송신된 정보 및 데이터를 해독한다.

데이터를 송신하기 전에 데이터 송신기(2)에 의해 행해지는 단계들 및 데이터를 수신한 후에 데이터 수신기(3)에 의해 행해지는 단계들을 하기에 설명한다. 데이터 송신기(2)가 데이터를 송신하기 전에 수행하는 단계들은 도 12의 흐름도에 예시적으로 도시되어 있다. 데이터 수신시 상기 데이터 수신기(3)에 의해 행해지는 단계들은 도 14의 흐름도에 예시적으로 도시되어 있다.

도 12의 단계(S21)에서, 데이터 송신기(2)는 송신기 그 자체 또는 양방향 통신 채널(9)에 접속되어 있는 인터페이스로부터 데이터 수신기(3)로 송신될 IP 데이터그램을 수신한다. 데이터 송신기(2)는 또한 인터넷(6)으로부터의 억세스 정보에 의거하여 정보 센터로부터 정보를 수신한다.

단계 S22에서, 상기 데이터 송신기(2)는 IP 데이터그램의 행선 어드레스부를 검사하여 제 1 프로토콜에 의거한 행선 어드레스를 찾아낸다. 예를 들면, 상기 데이터 송신기(2)는 도 13에 도시된 것과 같이 데이터 송신기(2)에 포함되어 있는 **IP** 어드레스와 **MAC** 어드레스 대응표를 참조하여 제 1 프로토콜에 따라서 데이터 수신기(3)의 행선 어드레스를 찾아낸다.

이렇게 찾아낸 행선 어드레스를 이용하여, 상기 데이터 송신기(2)는 상기 행선 어드레스에 따라서 섹션을 생성한다. 여기서, 데이터 송신기(2)는 필요한 경우 상기 데이터부에 "1"에 의한 패딩을 행하며, 따라서 상기 데이터부는 64 비트의 배수가 된다.

단계 S23에서, 데이터 송신기(2)는 도 11에 도시된 **MAC** 어드레스와 세션 키 대응표에서 키(Ks)의 플래그(112)를 검사하므로서 현재 사용된 세션 키(Ks)를 추출한다. 데이터 송신기(2)는 상기 추출된 세션 키(Ks)를 이용하여 도 7c에 도시된 섹션의 데이터부를 암호화한다. 여기서, 데이터 송신기(2)는 현재의 세션 키(Ks)의 플래그를 검사하여 그 플래그의 내용을 도 11에 도시된 세션 **헤더**의 psc(111)의 상위 비트로 설정한다.

단계 S24에서, 도 7e 내지 7g에 도시된 바와 같이, 상기 데이터 송신기(2)는 전체 섹션(109)을 TS 패킷(106, 107, 108)의 **페이로드** 부분들(P)로 분할한다. 상기 TS 패킷(106, 107, 108)에는 미리 정해진 PID가 각각 부가된다. 상기 **페이로드**(P)는 위성 링크(4a)로 출력되기 전에 제 2 프로토콜에 의해 요구된 바와 같이 암호화된다.

이상 데이터 송신기(2)의 데이터 송신 전의 준비 단계를 설명하였다. 위성 링크(4a)를 통해 수신된 데이터를 갖는 데이터 송신기(3)는 하기의 단계들을 수행한다.

도 14의 단계 S31에서, 데이터 수신기(3)는 위성 링크(4a)를 통해 수신한 TS 패킷(106, 107, 108)을 해독하여 전체 섹션(109)을 재구성한다.

단계 S32에서, 데이터 수신기(3)는 상기 섹션의 행선 어드레스(즉, **MAC** 어드레스)를 추출한다. 단계 S33에서, 데이터 수신기(3)는 **MAC** 어드레스가 도 15에 도시된 **MAC** 어드에스와 세션 키 대응표에 있는지 검사한다. 즉, 상기 섹션이 데이터 수신기(3)가 수신하도록 허가된 데이터를 포함하는지의 여부가 검사된다. **MAC** 어드레스가 단계 S33에서 발견되지 않으면, 데이터 수신기(3)는 단계 S34로 진행하여 상기 데이터를 폐기한다. **MAC** 어드레스가 검출되면, 상기 데이터 수신기(3)는 도 10에 도시된 psc(111)가 섹션 **헤더**(103)로부터 추출되는 단계 S35로 진행한다. 데이터 수신기(3)는 psc(111)의 상위 비트를 검사하여 두 개의 세션 키(Ks)중 어느 키가 현재 유효한지 파악하여, 유효한 세션 키(Ks)를 선택한다.

단계 S36에서, 상기 데이터 수신기(3)는 트리플 DES에 따라서 검색된 세션키(Ks)를 이용하여 섹션 데이터(104)를 해독한다. 단계 S37에서, 데이터 수신기(3)는 상기 해독된 데이터로부터 IP 데이터그램을 추출한다. 예를 들면, 데이터 수신기(3)는 상기 해독된 데이터부 앞에 놓인 **IP 헤더**로부터 총 길이 필드(113)(도 16)를 판독하고, 그 필드(113)로부터 IP 데이터그램의 길이를 찾아내어 그에 따라서 계산된 전체 IP 데이터그램을 추출한다. 상기 과정에서, 암호화시에 부가된 과도한 패딩이 제거되어 타겟 IP 데이터그램이 그대로 추출된다.

전술한 단계들을 수행하므로서, 데이터 송신기(2)는 데이터 송신 전에 필요한 처리를 행하고, 데이터 수신기(3)는 상기 수신된 데이터와 관련된 처리를 행한다. 따라서 데이터 수신기(3)는 그 수신기로 어드레스된 정보 및 데이터를 받아들인다.

전술한 바와 같이 구성된 데이터 전송 시스템(1)은 앞에서 언급한 종래의 문제점들을 해결할 수 있다.

상기 데이터 전송 시스템(1)은 또한 수정될 수도 있다. 도 17은 상기 시스템(1)의 제 1 변형인 데이터 전송 시스템(201)이다. 상기 데이터 전송 시스템(201)은 상기 데이터 수신기(3)가 IP 라우터를 구비하고 있다는 것을 특징으로 한다.

상기 데이터 전송 시스템(1)은 IP 데이터그램을 직접 수신하는 데이터 수신기(3a)를 가진다. 반면에 데이터 송신 시스템(201)은 IP 라우터로서 구성된 데이터 수신기(3a)를 가진다. 이 구성에 의해 위성 링크(4a)로부터 데이터 수신기(3a)에 의해 수신된 데이터는 상기 위성 링크(4a)와 인터페이스되지 않는 컴퓨터(203a 및 203b)로 전송될 수 있으며, 상기 컴퓨터(203a 및 203b)는 이더넷과 같은 로컬 에리어 네트워크(LAN)를 통해 데이터 수신기(3a)에 접속된다. 이 경우, 데이터 송신기(2) 및 데이터 수신기(3a)는 상기 데이터 수신기(3a)와 상기 데이터 수신기(3a)에 접속된 로컬 에리어 네트워크(202) 상에 있는 모든 컴퓨터(203a 및 203b)를 통하여 데이터 한정 수신 제어를 할 수 있다. 특히, 데이터 송신기(2)의 IP 어드레스들이 섹션 헤션 어드레스들(MAC 어드레스들)과 대응하도록 설정되는 도 13의 대응표 내에서, 각각의 IP 어드레스들은 복수의 IP 어드레스들을 각각 나타내는 IP 네트워크 어드레스들과 치환된다. 데이터 수신기(3a)와 컴퓨터(203a 및 203b) 사이의 데이터 한정 전송 제어를 위해서는 IP 프로토콜 또는 상위 애플리케이션의 레벨에서의 데이터 한정 전송 제어 방법이 요구된다. 이것은 데이터 전송 시스템(201)에서의 데이터 전송이 위성 링크(4a)를 통해서만 행해지기 때문이다.

상기 시스템(1)의 제 2 변형인 데이터 전송 시스템(301)이 도 18에 도시되어 있다. 상기 데이터 전송 시스템(301)에서, 데이터 수신기(3a)는 IP 데이터그램을 회송하는데 있어서 프로토콜 변환을 전적으로 행하는 브리지로서 구성된다. 상기 데이터 전송 시스템(301)은 상기 시스템(301)이 루팅을 행하지 않는다는 점에 있어서 상기 시스템(201)과 상이하다.

상기 데이터 수신기(3a)는 위성 링크(4a)를 통해 수신한 데이터를 해독하여 IP 데이터그램을 추출한다. 상기 추출된 IP 데이터그램은 이더넷 프레임에 배치되어 범용 라우터(302)로 전송된다. 차례대로 라우터(302)는 IP 데이터그램에 대하여 일반적인 처리를 행한다. 데이터 수신기(3a)는 자신에 대한 루팅을 행할 필요없이 단순하게 구성되고 범용 라우터와 함께 사용된다.

본 발명의 정신 및 범주를 벗어나지 않고 본 발명에 대한 많은 다른 실시예들이 이루어질 수도 있으므로, 본 발명은 첨부한 청구범위에 정의된 것을 제외한 특정 실시예들에 한정되지 않음을 주지하라.

발명의 효과

이상과 같이 본 발명에 의하면 데이터 송신기로부터 데이터 수신기로의 데이터 전송에 있어서, 보다 더 안전하고 확실하게 데이터를 전송할 수 있다.

(57) 청구의 범위

청구항 1

데이터 송신 수단으로부터 통신 채널을 통하여 데이터 수신 수단으로의 데이터 전송 제어 방법에 있어서,

상기 데이터 송신 수단에 의해 암호화된 데이터를, 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 데이터 전송을 위해 제공된 제 1 통신 채널을 통해 상기 데이터 수신 수단으로 전송하는 단계와,

상기 암호화된 데이터가 적어도, 상기 제 1 통신 채널보다 더 적은 데이터 전송량을 가지며 또한 상기 데이터 수신 수단으로부터 상기 데이터 송신 수단으로의 데이터 전송에 사용되는 제 2 통신 채널을 통해, 특정 데이터 수신 수단에 의해서만 수신되도록 데이터 한정 전송 제어 정보를 상기 데이터 수신 수단으로 전송하는 단계를 포함하는 데이터 전송 제어 방법.

청구항 2

제 1항에 있어서, 상기 제 2 통신 채널은 상기 데이터 송신 수단과 상기 데이터 수신 수단 사이에서 양방향 통신을 허용하는 통신 채널인 데이터 전송 제어 방법.

청구항 3

제 1항에 있어서, 상기 데이터 송신 수단은 암호화 키를 사용하여 데이터 암호화를 행하고, 상기 데이터 송신 수단으로부터 상기 암호화된 데이터는 상기 데이터 암호화에 사용된 상기 암호화 키와 등일한 암호 해독 키를 이용하여 상기 데이터 수신 수단에 의해 해독되는 데이터 전송 제어 방법.

청구항 4

제 3항에 있어서, 상기 암호화 키 및 상기 암호 해독 키는 정보 및 데이터를 암호화 및 해독하는 세션 키인 데이터 전송 제어 방법.

청구항 5

제 4항에 있어서, 상기 세션 키는 소정 간격으로 갱신되는 데이터 전송 제어 방법.

청구항 6

제 4항에 있어서, 상기 데이터 송신 수단 및 상기 데이터 수신 수단은 상기 데이터 수신 수단 고유의 마스터 키를 가지며,

상기 데이터 송신 수단은 상기 마스터 키를 이용하여 상기 세션 키를 암호화하여, 상기 암호화된 세션 키를 상기 제 1 통신 채널 또는 상기 제 2 통신 채널을 통하여 상기 데이터 수신 수단으로 전송하고,

상기 데이터 수신 수단은 상기 마스터 키를 이용하여 수신된 상기 암호화된 세션 키를 해독하는 데이터 전송 제어 방법.

청구항 7

제 6항에 있어서, 상기 데이터 송신 수단은 특정 정보 및 데이터를 수신하도록 허가된 모든 데이터 수신 수단에 대응하는 상기 세션 키를 가지며,

상기 데이터 송신 수단은 사전에 상기 세션 키를 특정 정보 및 데이터를 수신하도록 허가된 상기 데이터 수신 수단에 전송하는 데이터 전송 제어 방법.

청구항 8

제 1항에 있어서, 상기 제 1 통신 채널은 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 양방향 통신을 허용하는 위성 링크이고,

상기 제 2 통신 채널은 상기 데이터 송신 수단과 상기 데이터 수신 수단 사이에서 양방향 통신을 하는 통신 채널인 데이터 전송 제어 방법.

청구항 9

제 1항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되어 있는 데이터 전송 제어 방법.

청구항 10

제 1항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되어 있는 데이터 전송 제어 방법.

청구항 11

데이터 전송 시스템에 있어서,

데이터를 암호화하고 상기 암호화된 데이터를 송신하는 데이터 송신 수단과,

상기 데이터 송신 수단으로부터 상기 암호화된 데이터를 수신하는 데이터 수신 수단과,

상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 데이터 전송에 사용된 제 1 통신 채널과,

데이터 수신 수단으로부터 상기 데이터 송신 수단으로의 데이터 전송에 또한 사용되며, 상기 제 1 통신 채널보다 더 적은 데이터 전송량을 갖는 제 2 통신 채널을 포함하고,

상기 제 1 통신 채널은 상기 암호화된 데이터를 전송하는데 사용되고,

적어도 상기 제 2 통신 채널은 상기 암호화된 데이터가 특정 데이터 수신 수단에 의해서만 수신되도록 데이터 한정 전송 제어 정보를 전송하는데 사용되는 데이터 전송 시스템.

청구항 12

제 11항에 있어서, 상기 데이터 송신 수단은 암호화 키를 사용하여 데이터 암호화를 행하고, 상기 데이터 송신 수단으로부터의 상기 암호화된 데이터는 상기 데이터 암호화에 사용된 상기 암호화 키와 동일한 암호 해독 키를 이용하여 상기 데이터 수신 수단에 의해 해독되는 데이터 전송 시스템.

청구항 13

제 12항에 있어서, 상기 암호화 키 및 상기 암호 해독 키는 정보 및 데이터를 암호화 및 해독하는 세션 키인 데이터 전송 시스템.

청구항 14

제 13항에 있어서, 상기 세션 키는 소정 간격으로 갱신되는 데이터 전송 시스템.

청구항 15

제 13항에 있어서, 상기 데이터 송신 수단 및 상기 데이터 수신 수단은 상기 데이터 수신 수단 고유의 마스터 키를 가지며,

상기 데이터 송신 수단은 상기 마스터 키를 이용하여 상기 세션 키를 암호화하여 상기 암호화된 세션 키를 상기 제 1 통신 채널 또는 상기 제 2 통신 채널을 통하여 상기 데이터 수신 수단으로 전송하고,

상기 데이터 수신 수단은 상기 마스터 키를 이용하여 수신된 상기 암호화된 세션 키를 해독하는 데이터 전송 시스템.

청구항 16

제 15항에 있어서, 상기 데이터 송신 수단은 특정 정보 및 데이터를 수신하도록 허가된 모든 데이터 수신 수단에 대응하는 상기 세션 키를 가지며,

상기 데이터 송신 수단은 미리 상기 세션 키를 특정 정보 및 데이터를 수신하도록 허가된 상기 데이터 수신 수단에 전송하는 데이터 전송 시스템.

청구항 17

제 11항에 있어서, 상기 제 1 통신 채널은 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 양방향 통신을 허용하는 위성 링크인 데이터 전송 시스템.

청구항 18

제 11항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되어 있는 데이터 전송 시스템.

청구항 19

제 11항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되어 있는 데이터 전송 시스템.

청구항 20

데이터 송신 수단으로부터 통신 채널을 통하여 데이터 수신 수단으로의 데이터 전송을 제어하고, 상기 데이터 송신수단의 데이터를 암호화하여 상기 통신 채널을 통해 상기 데이터 수신 수단으로 전송하도록 하는 데이터 전송 제어 방법에 있어서,

복수의 프로토콜에 따라서 데이터를 멀티플렉스된 형태로 전송하도록 캡슐화하는 단계와,

상기 캡슐화에 의한 데이터 캡슐들 중 적어도 하나를 암호화하는 단계를 포함하는 데이터 전송 제어 방법.

청구항 21

제 20항에 있어서, 상기 데이터 캡슐화 단계는 제 1 프로토콜에 따라서 상기 데이터 수신 수단으로 전송될 데이터를 캡슐화하는 제 1 캡슐화 단계와,

제 2 프로토콜에 따라서 상기 제 1 캡슐 단계로부터 캡슐화된 데이터를 한번 더 캡슐화하는 제 2 캡슐화 단계를 포함하고,

상기 제 1 캡슐화 단계는 상기 데이터 수신 수단으로 전송되는 상기 데이터를 포함하는 실데이터부(real data part)에 상기 실데이터부와 관련된 부가적인 정보를 부가하고 상기 제 1 캡슐화 단계는 상기 실데이터부를 다시 암호화하는 데이터 전송 제어 방법.

청구항 22

제 21항에 있어서, 상기 부가적인 정보부는 상기 실데이터부에 포함된 데이터를 수신하도록 허가된 데이터 수신 수단을 나타내는 행선 어드레스 정보를 포함하는 데이터 전송 제어 방법.

청구항 23

제 22항에 있어서, 상기 행선 어드레스 정보는 개별적인 행선 어드레스 정보 또는 그룹 행선 어드레스 정보인 데이터 전송 제어 방법.

청구항 24

제 22항에 있어서, 상기 데이터 송신 수단은 상기 행선 어드레스 정보에 대응하는 세션 키를 포함하며, 상기 세션 키는 정보 및 데이터를 암호화하기 위해 상기 데이터 송신 수단에 의해 사용되고, 수신된 상기 암호화된 정보 및 데이터를 해독하기 위해 상기 수신 수단에 의해 사용되고,

상기 데이터 송신 수단은 사전에 상기 세션 키를 상기 행선 어드레스 정보에 따라서 상기 전송된 정보 및 데이터를 수신하도록 허가된 상기 데이터 수신 수단으로 전송하는 데이터 전송 제어 방법.

청구항 25

제 24항에 있어서, 상기 세션 키는 소정의 간격으로 갱신되는 데이터 전송 제어 방법.

청구항 26

제 24항에 있어서, 상기 세션 키는 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로의 일방향 통신 또는 이들간의 양방향 통신을 허용하는 통신 채널을 통해 전송되는 데이터 전송 제어 방법.

청구항 27

제 21항에 있어서, 상기 제 1 캡슐화 단계는 상기 실데이터부에 부가된 상기 행선 어드레스 정보가 상기 부가적인 정보부에 기억되는 방법을 유일하게 판정하고, 상기 제 1 캡슐화 단계는 상기 행선 어드레스 정보에 대응하는 상기 데이터수신 수단 고유의 마스터 키를 이용하여 상기 실데이터부를 다시 암호화하는 데이터 전송 제어 방법.

청구항 28

제 22항에 있어서, 상기 부가적인 정보부는 상기 행선 어드레스 정보를 제공하는 48 비트 공간을 제공하는 데이터 전송 제어 방법.

청구항 29

제 21항에 있어서, 상기 제 1 캡슐화 단계는 인터넷 프로토콜 또는 이더넷 프로토콜에 따라서 상기 데이터 수신 수단으로 전송되는 데이터를 캡슐화하는 데이터 전송 제어 방법.

청구항 30

제 20항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되는 데이터 전송 제어 방법.

청구항 31

제 20항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되는 데이터 전송 제어 방법.

청구항 32

데이터 송신 수단으로부터 통신 채널을 통한 데이터 수신 수단으로의 데이터 전송을 제어하고 상기 데이터 송신 수단이 데이터를 암호화하여 상기 암호화된 데이터를 상기 통신 채널을 통해 상기 데이터 수신 수단으로 전송하도록 하는 데이터 송신 제어 방법에 있어서,

암호화 키를 사용하여 데이터를 암호화하는 단계와,

상기 암호화된 데이터에 상기 암호화 키에 대한 암호화 키 정보를 부가하는 단계와,

상기 암호화 키 정보와 함께 상기 암호화된 데이터를 상기 데이터 송신 수단으로부터 상기 데이터 수신 수단으로 전송하는 단계와,

상기 데이터 수신 수단이 상기 암호화된 데이터를 해독하도록 하고 자주 갱신되는 복수의 암호 해독 키 중 하나의 해독 키를 이용하여 상기 암호화된 데이터를 해독하고, 상기 하나의 암호 해독 키는 상기 암호화된 정보에 부가된 상기 암호화 키 정보에 따라서 선택되는 데이터 전송 제어 방법.

청구항 33

제 32항에 있어서, 상기 복수의 암호 해독 키는 수신된 상기 암호화된 데이터를 해독하기 위해 현재 사용 가능한 암호 해독 키와 상기 수신된 암호화된 데이터를 해독하기 위해 다음에 사용되는 암호 해독 키를 포함하고,

상기 데이터 해독 단계는 상기 암호화 키 정보에 의거하여 현재 사용 가능한 암호 해독 키를 선택하는 데이터 전송 제어 방법.

청구항 34

제 33항에 있어서, 상기 암호화 키 및 상기 암호 해독 키는 정보 및 데이터를 암호화하는 세션 키인 데이터 전송 제어 방법.

청구항 35

제 34항에 있어서, 상기 세션 키는 소정 간격으로 갱신되는 데이터 전송 제어 방법.

청구항 36

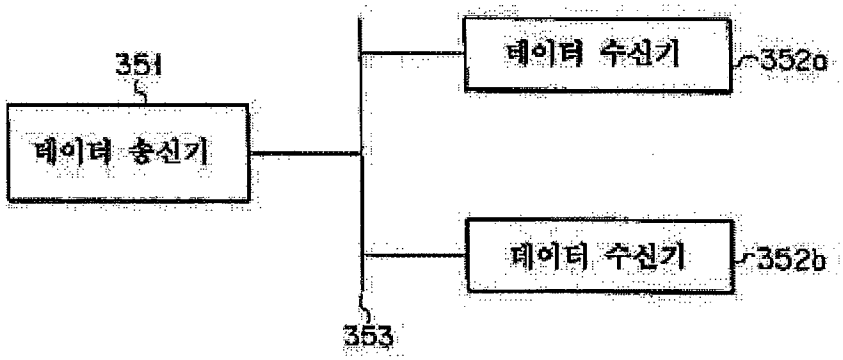
제 32항에 있어서, 상기 데이터 수신 수단은 IP 라우터로서 구성되는 데이터 전송 제어 방법.

청구항 37

제 32항에 있어서, 상기 데이터 수신 수단은 브리지로서 구성되는 데이터 전송 제어 방법.

도면

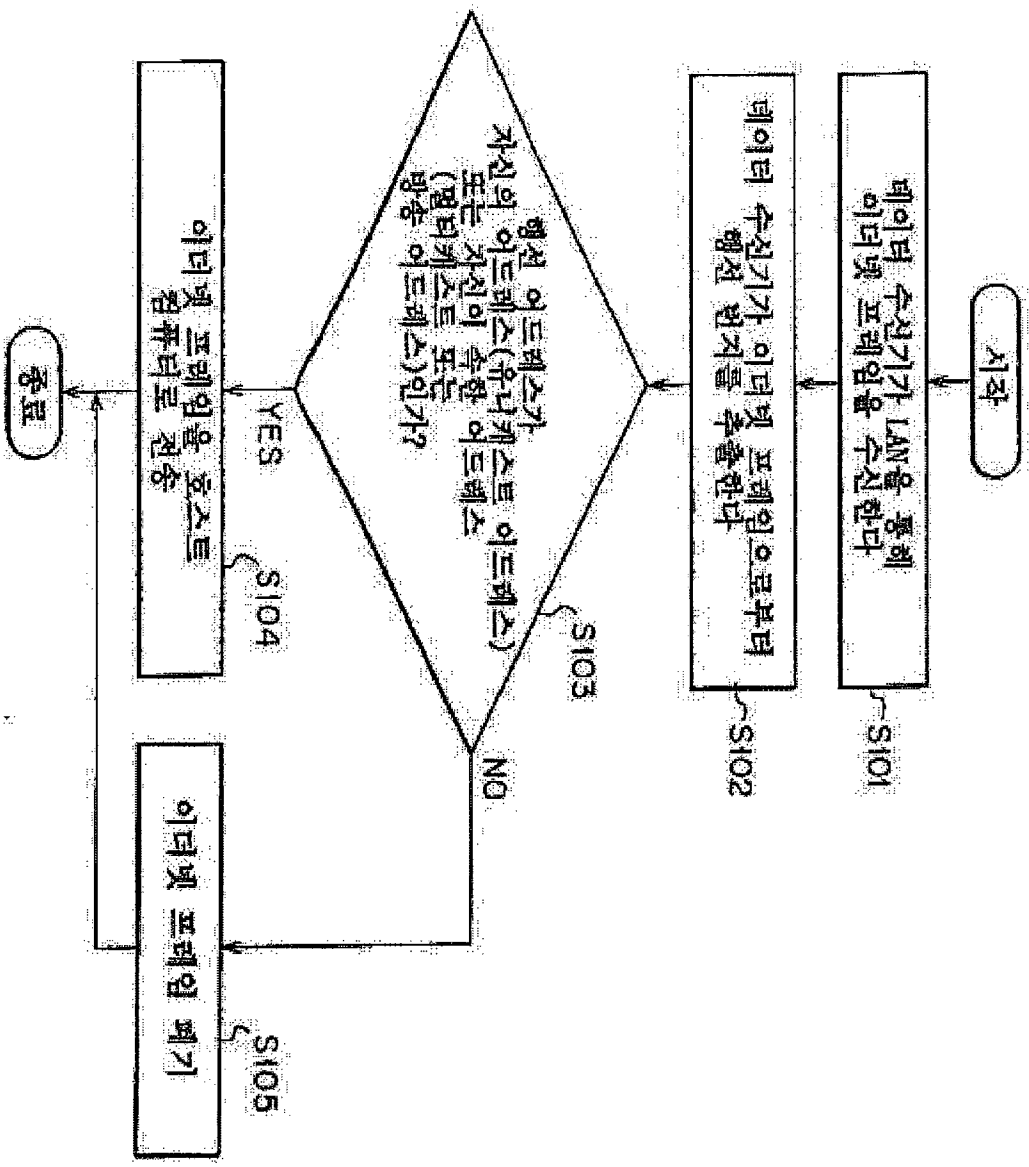
도면1



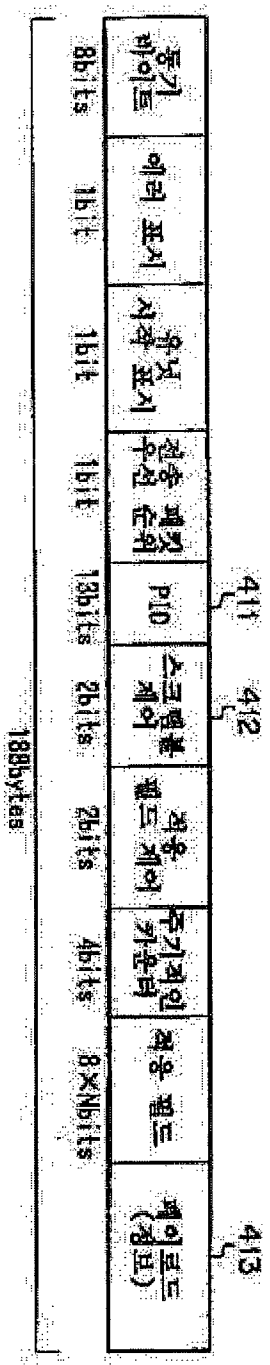
도면2

401
프리앰블
8 octets
목적지 어드레스
6 octets
소스 어드레스
6 octets
길이/타입
2 octets
프레임 페이로드
64-1500 octets
CRC
4 octets

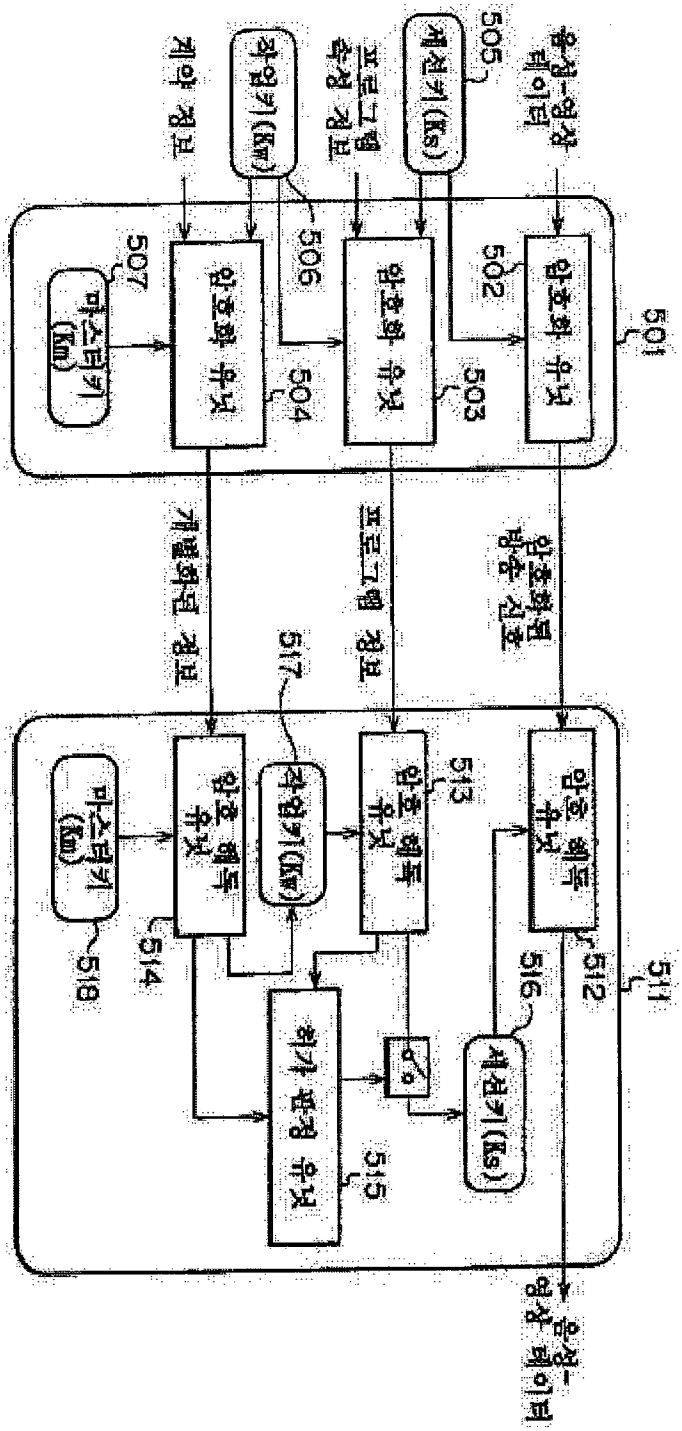
도면3


시작
데이터 수신기가 LAN을 통해 이더넷 프레임을 수신한다
S101
데이터 수신기가 이더넷 프레임으로부터 헤더 부분을 추출한다
S102
헤더 부분의 어드레스가 자신의 또는 (멀티캐스트 방송 어드레스)인가?
S103
YES
NO
이더넷 프레임을 호스트 컴퓨터로 전송
S104
이더넷 프레임 폐기
S105
종료

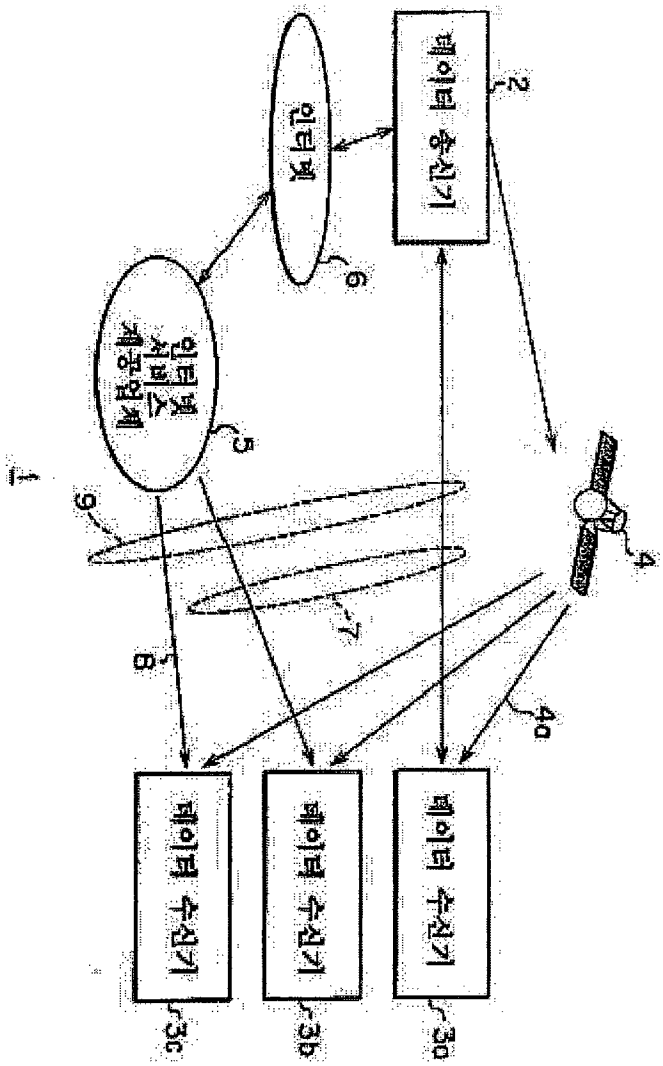
도면4


동기 바이트
8bits
에러 표시
1bit
유닛 시작 표시
1bit
전송 우선 순위
1bit
PID
13bits
411
스크램블 제어
2bits
412
적응 필드 제어
2bits
연속 카운터
4bits
적응 필드
8×Nbits
페이로드 (정보)
413
188bytes

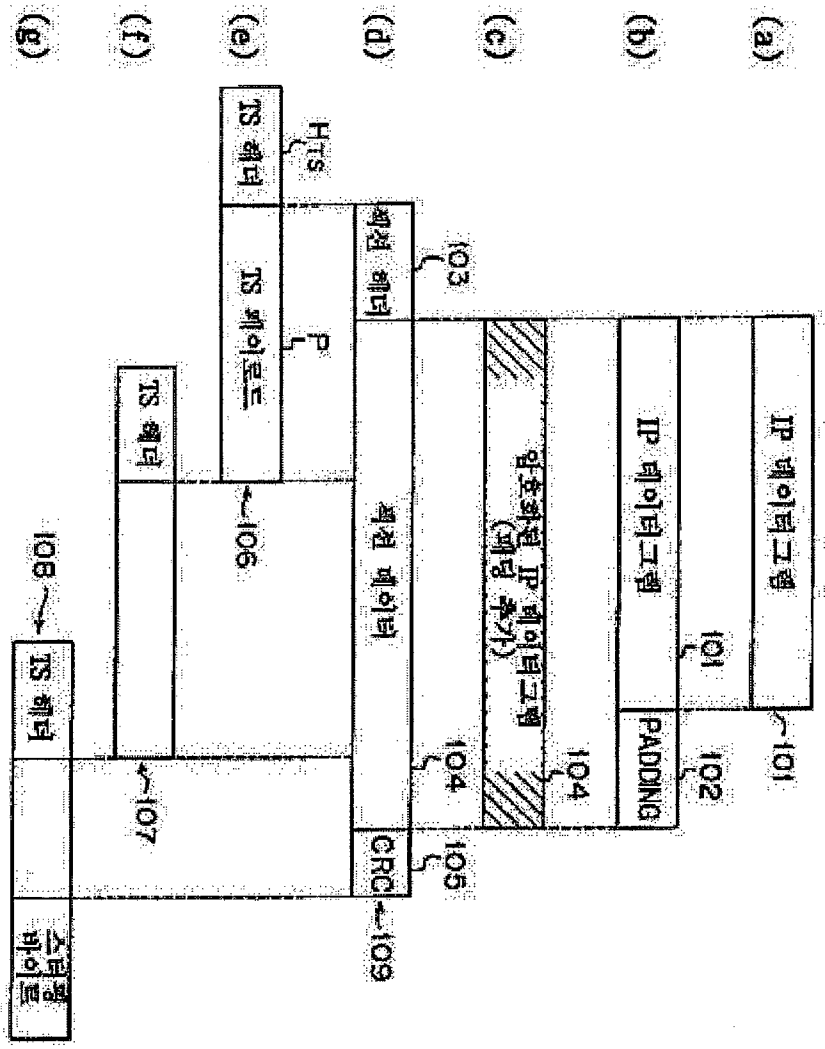
도면5


암호화 유닛
501
암호화 유닛
503
암호화 유닛
504
마스터키 (Km)
507
세션키(Ks)
505
작업키(Kw)
506
암호화 유닛
502
음성-영상 데이터
제어 정보
프로그램 정보
암호화된 음성 신호
개별화된 정보
프로그램 정보
암호화된 음성 신호
511
암호 해독 유닛
512
암호 해독 유닛
513
암호 해독 유닛
514
작업키(Kw)
517
마스터키 (Km)
518
세션키(Ks)
516
키 발생 유닛
515
음성-영상 데이터

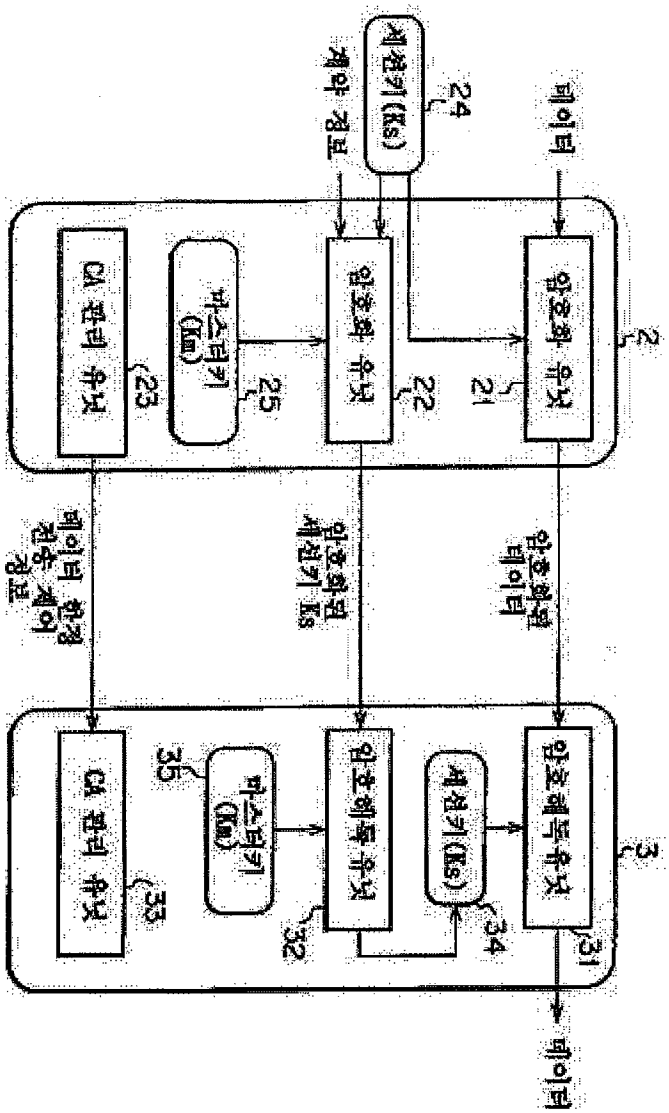
도면8


1
2
데이터 송신기
인터넷
6
인터넷 서비스 제공업체
5
9
7
8
4
4a
데이터 수신기
3c
데이터 수신기
3b
데이터 수신기
3a

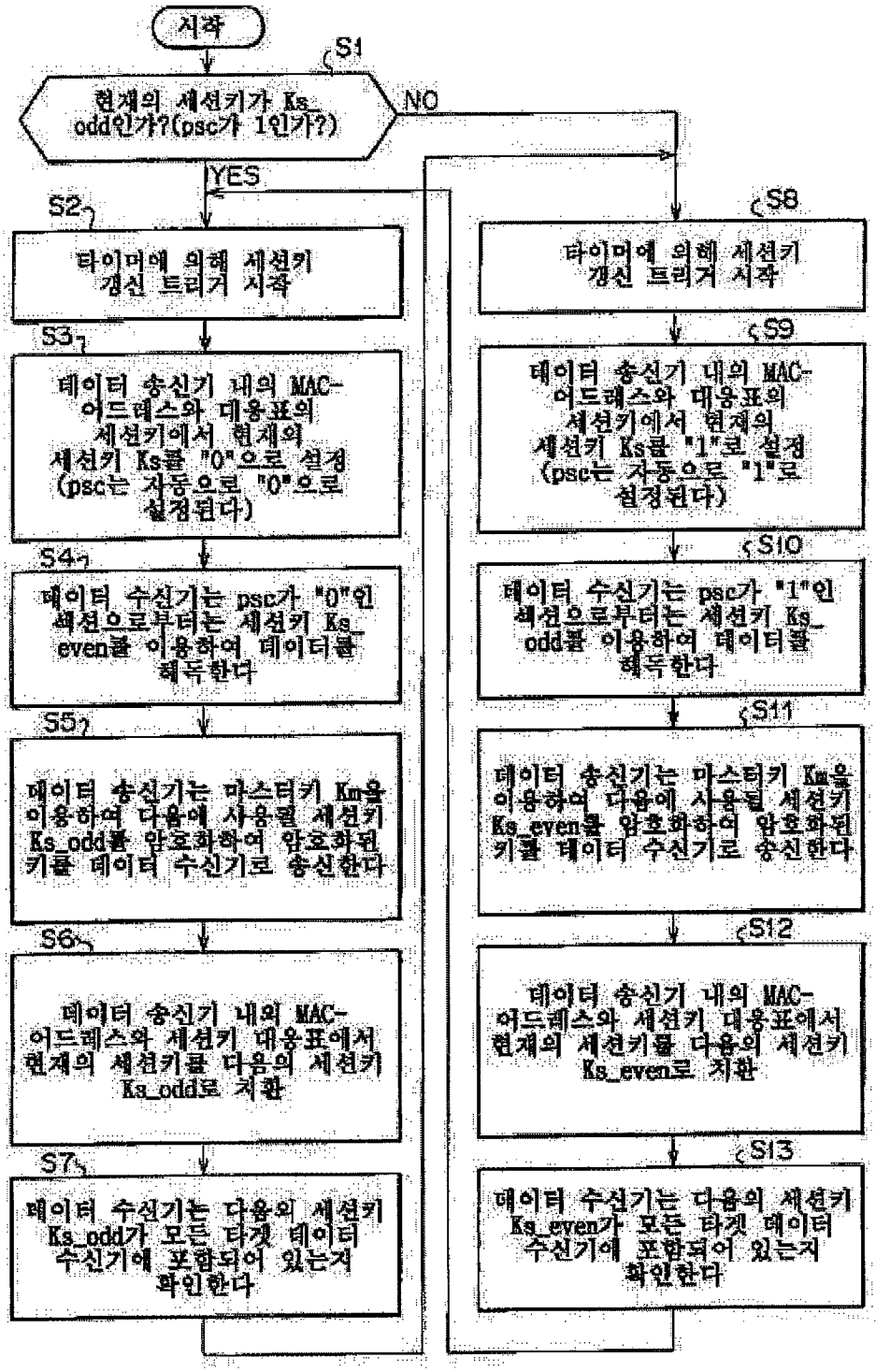
도면7


(a)
(b)
(c)
(d)
(e)
(f)
(g)
IP 데이터그램
101
IP 데이터그램
PADDING
102
암호화된 IP 데이터그램
(패딩 추가)
104
헤더 삽입
CRC
105
헤더
103
TS 헤더
TS 페이로드
P
HTS
106
TS 패킷
107
TS 패킷
스트림 바이트
108
109

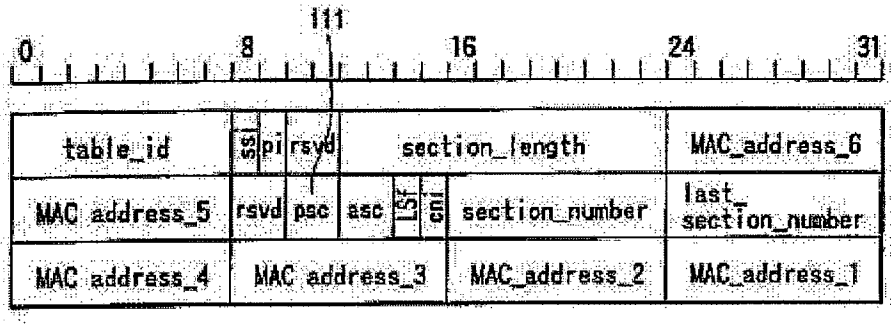
도면8


세션키(Ks)
24
제어 정보
데이터
암호화 유닛
2
21
암호화 유닛
22
마스터키 (Km)
25
CA 관리 유닛
23
데이터 전송 제어 정보
암호화된 세션키 Ks
암호화된 데이터
암호해독 유닛
3
31
세션키(Ks)
34
암호해독 유닛
32
마스터키 (Km)
35
CA 관리 유닛
33
데이터

도면9


시작
S1
현재의 세션키가 Ks_odd인가?(psc가 1인가?)
NO
YES
S2
타이머에 의해 세션키 갱신 트리거 시작
S3
데이터 송신기 내의 MAC-어드레스와 대응표의 세션키에서 현재의 세션키 Ks를 "0"으로 설정 (psc는 자동으로 "0"으로 설정된다)
S4
데이터 수신기는 psc가 "0"인 세션으로부터는 세션키 Ks_even를 이용하여 데이터를 해독한다
S5
데이터 송신기는 마스터키 Km을 이용하여 다음에 사용될 세션키 Ks_odd를 암호화하여 암호화된 키를 데이터 수신기로 송신한다
S6
데이터 송신기 내의 MAC-어드레스와 세션키 대응표에서 현재의 세션키를 다음의 세션키 Ks_odd로 치환
S7
데이터 수신기는 다음의 세션키 Ks_odd가 모든 타겟 데이터 수신기에 포함되어 있는지 확인한다
S8
타이머에 의해 세션키 갱신 트리거 시작
S9
데이터 송신기 내의 MAC-어드레스와 대응표의 세션키에서 현재의 세션키 Ks를 "1"로 설정 (psc는 자동으로 "1"로 설정된다)
S10
데이터 수신기는 psc가 "1"인 세션으로부터는 세션키 Ks_odd를 이용하여 데이터를 해독한다
S11
데이터 송신기는 마스터키 Km을 이용하여 다음에 사용될 세션키 Ks_even를 암호화하여 암호화된 키를 데이터 수신기로 송신한다
S12
데이터 송신기 내의 MAC-어드레스와 세션키 대응표에서 현재의 세션키를 다음의 세션키 Ks_even로 치환
S13
데이터 수신기는 다음의 세션키 Ks_even가 모든 타겟 데이터 수신기에 포함되어 있는지 확인한다

도면10



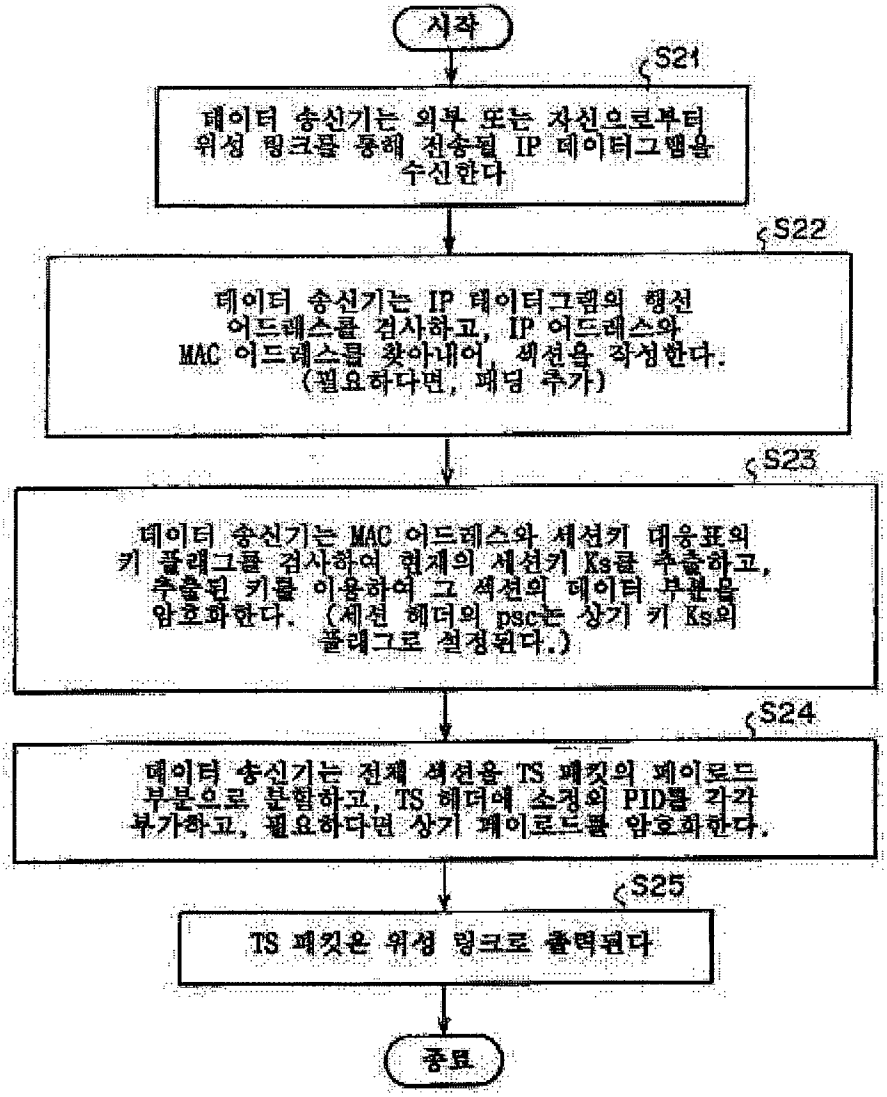
ssi : section_syntax_indicator
pi : private_indicator
rsvd : reserved
psc : payload_scramble_indicator
asc : address_scramble_indicator
LSf : LLC_SNAP_flag
cni : current_next_indicator

도면11

112

MAC 어드레스	Ks_even	Ks_odd	Ks 플래그
08:00:46:01:07:24	0×C08F...25	0×90B3...AF	0
08:00:45:01:07:09	0×2602...61	0×8A02...3C	1
01:00:5e:16:0:0	0×461E...67	0×DC1A...22	0

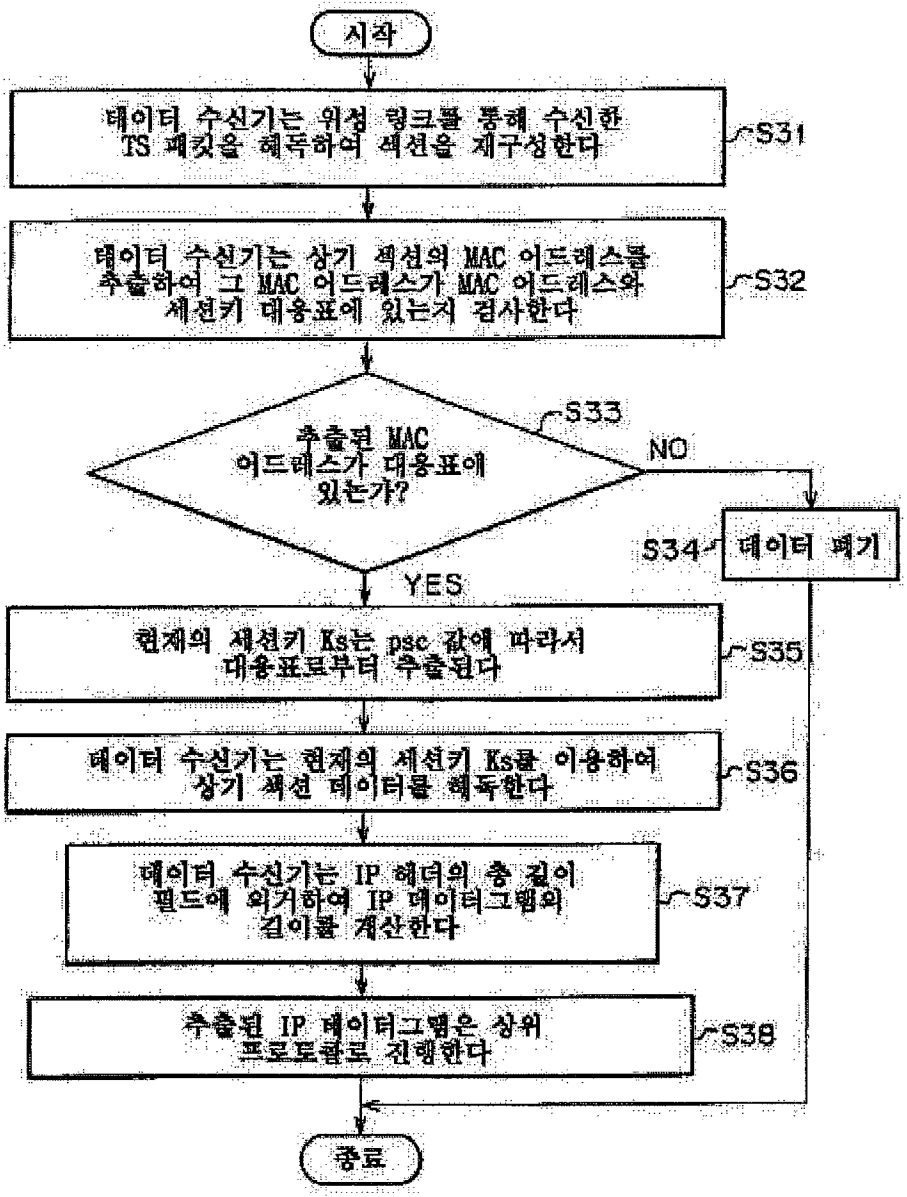
도면12



도면13

IP 어드레스	bitmask	MAC address
133.11.9.39	255.255.255.225	08:00:46:01:07:24
133.11.20.0	255.255.255.0	08:00:46:01:07:09
226.0.0.0	255.255.255.224	01:00:5e:16:0:0

도면14



도면15

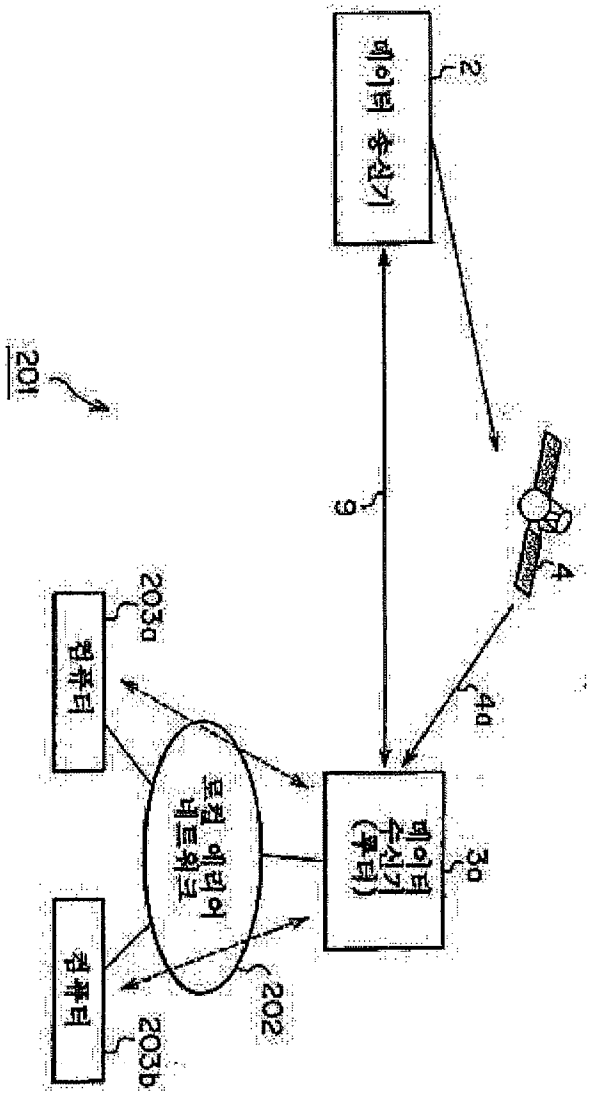
MAC 어드레스	Ks_even	Ks_odd
08:00:46:01:07:24	0×C08F...25	0×9083...AF
01:00:5e:16:0:0	0×461E...67	0×DC1A...22

도면16

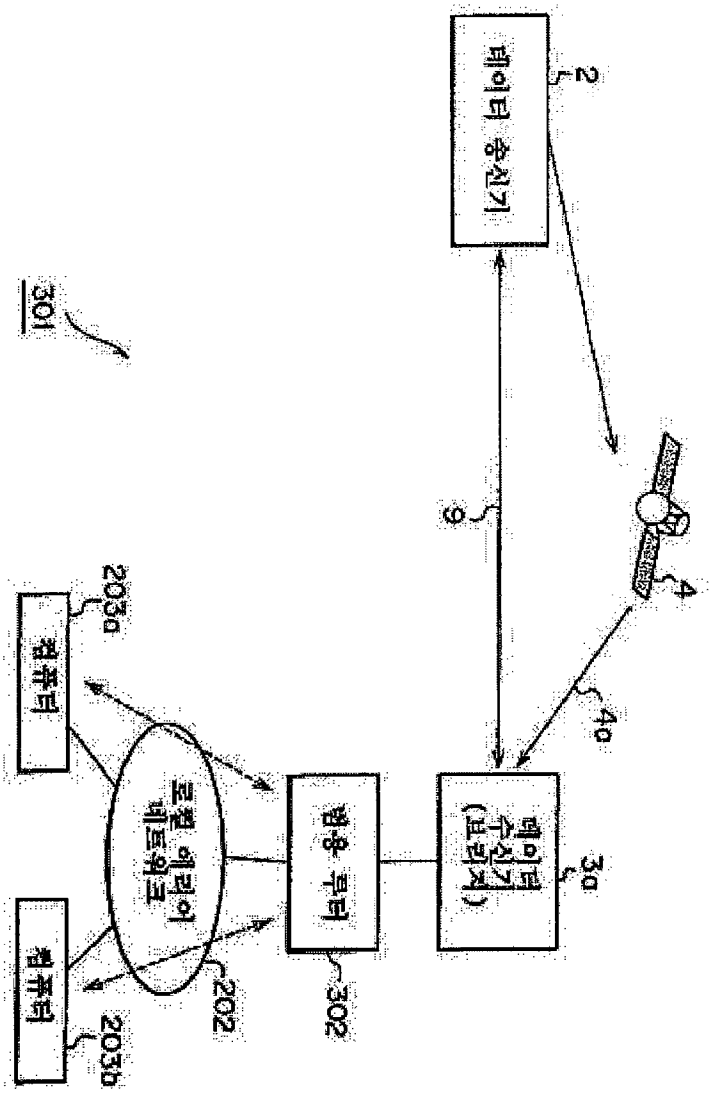
113

VERS	HLEN	SERVIE TYPE	TOTAL LENGTH
IDENTIFICAION		FLAGS	FRAGMENT OFFSET
TIME TO LIVE	PROTOCOL		HEADER CHECKSUM
SOURCE IP ADDRESS			
DESTINATION IP ADDRESS			
IP OPTIONS (IF ANY)			PADDING
DATA			
. . . . .			

도면17



도면18


301
데이터 송신기
2
6
4
40
데이터 수신기 (RT)
30
라우터
302
로컬 에리어 네트워크
202
컴퓨터
203a
컴퓨터
203b